



Digital Forensics Acquisition Process With FTK Imager

Aung Zaw Myo (Third Eye)

www.forensicsmyanmar.com

ယခုရေးသားတဲ့ Digital Forensics Acquisition Process With FTK Imager အကြောင်းမှာ အခုမှ ဖတ်တဲ့သူတွေ ပိုပြီးနားလည်သဘောပေါက်စေရန်အတွက် eCDFP Module (2) မှာပါတဲ့ Forensics Acquisition Process အကြောင်းကို ဦးစွာ ဖော်ပြထားပါတယ်။ Blog မှာလဲ ယခု အကြောင်းအရာနဲ့ပတ်သတ်ပြီး အရင်ကလဲများစွာဖော်ပြ ထားဖူးပါတယ်။

Data Acquisition

ကျွန်တော်တို့ Information Security မှာလိုပဲ Digital Forensics လုပ်မယ်ဆိုရင် Investigator က အရင်ဆုံး Data တွေကို Collect လုပ်ရပါတယ်။ Investigator အနေနဲ့ လုပ်ငန်းခွင်မှာ Evidence နဲ့ပတ်သတ်တဲ့ System/Storage တွေကိုကိုင် တွယ်ရတာ မျိုးရှိလာပါမယ်။ System/ Storage က Suspect သို့မဟုတ် Victim ရဲ့ ပစ္စည်းဖြစ်နိုင်ပါတယ်။ ကျွန်တော်တို့ အနေနဲ့ မူရင်း System/ Storage ကို ဥပဒေပိုင်းအရဆောင်ရွက် ရမှာဖြစ် တဲ့အတွက် System ကိုတိုက်ရိုက် Analysis မပြုလုပ်ပါ။ ဒါပေမဲ့ဒါကလဲ နိုင်ငံတွေအလိုက် ကွာခြားမှုတွေရှိနိုင်ပါတယ်။

What Is Acquisition?

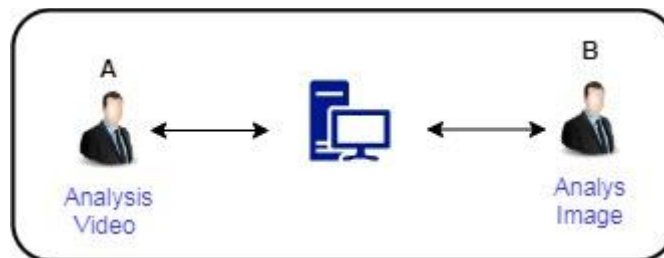
Acquisition ဆိုသည်မှာ Evidence Device တွေကို Forensics Copy ပြုလုပ်ခြင်းဖြစ်ပါတယ်။ Evidence Device တွေက (Hard Disk, USB, Etc ...) တွေဖြစ်နိုင်ပါတယ်။

Investigator က Analysis ပြုလုပ်ရင်းကြုံတွေ့လာနိုင်တဲ့ ပြဿနာတွေကို ရှောင်ရှားနိုင်ဖို့ အတွက် သူ Analysis ပြုလုပ်ရတဲ့ Physical System မှာ တိုက်ရိုက်လုပ်ဆောင်ခြင်းမရှိသင့်ပါ။ ဒါကြောင့် Investigator တွေက သူတို့ စစ်ဆေးမဲ့ System ရဲ့ Forensics Image ကိုရယူပြီး Analysis ပြုလုပ်ပါတယ်။ Forensics Image က System Storage အကုန်လုံးလဲ ဖြစ်နိုင်ပါတယ်။ ဒါကြောင့် Data Acquisition က System/machine ကနေ Image ရယူတဲ့ လုပ်ငန်းစဉ်ဖြစ်ပါတယ်။

Why Do We Acquire?

Investigator ကနေ ဘာလို့ Suspect ရဲ့ စက်ကို တိုက်ရိုက် Analysis မပြုလုပ် လုပ်ရတာ လဲဆိုတဲ့ အကြောင်းအရင်းများစွာရှိပါတယ်။

- Analysis ပြုလုပ်နေစဉ်အတွင်း Evidence ပျက်စီးနိုင်ခြင်း။
- အချို့သော Case များတွင် တစ်ဖက်မှ Analysis ပြီးဆုံးတဲ့အချိန်အထိ Evidence ပစ္စည်းကို မထားခဲ့နိုင်ခြင်း။
- System Down Time မပေးတဲ့ နေရာတွေ ဒါမှမဟုတ် သယ်ယူဖို့မလွယ်ကူတဲ့ System တွေကို စစ်ဆေးရမည့် အချိန်။ Server ကြီးတစ်ခုလုံးကို lab ကို ယူလာပြီး စစ်ဆေး ဖို့မလွယ်ကူပါဘူး။ (အခုအချိန်မှာတော့ Remote Acquisition နည်းလမ်းတွေရှိ လာနေပါပြီ။)
- မူရင်း Storage/ System တစ်ခုထဲဆိုရင် သက်ဆိုင်ရာအဖွဲ့အလိုက် ဒါမှမဟုတ် စစ်ဆေးတဲ့သူတွေက တစ်ပြိုင်ထဲ စစ်ဆေးဖို့မဖြစ်နိုင်ခြင်း။



ပုံမှာဆိုရင် System/Storage တစ်ခုထဲကိုပဲ A က Video File ကို စစ်ဆေးချင်တယ်။ B Image File ကို စစ်ဆေးနိုင်ချင်တယ်။ အဲလိုအနေအထားဆိုရင် Acquisition မပြုလုပ်ပဲ Analysis ပြုလုပ်မယ်ဆိုရင် မလွယ်ကူနိုင်ပါ။ (အခုနောက်ပိုင်းမှာတော့ Centralized နေရာမှာ Forensics Image ကိုထားပြီး လူအများကနေ ကိုယ်နဲ့သက်ဆိုင်ရာ အပိုင်းအလိုက်စစ်ဆေးတာတွေလဲ လုပ်နေကြပါပြီ။)

Forensics Image ပြုလုပ်တဲ့ အပိုင်းကိုမသွားခင်မှာ သတိထားရမဲ့ အချက်တွေကို သိထားဖို့လိုအပ်ပါတယ်။ မူရင်း System/Storage ကို တိုက်ရိုက် Analysis မလုပ်ဖို့နဲ့ ပထမ Forensics Image ကို Analysis မလုပ်ဖို့သတိပေးလိုပါတယ်။ ဘာလို့လဲဆိုရင် ပထမဆုံး Forensics Image က Verify ဖြစ်တဲ့အတွက်ကြောင့်ဖြစ်ပါတယ်။ Verify အကြောင်းကို နောက်ပိုင်းမှာ ရှင်းလင်းသွားပါမယ်။ နောက်ပြီး ပထမဆုံး Forensics Image ကို ပြုပြင်ပြောင်းလဲတာတွေမဖြစ်အောင်လဲ Protect ပြုလုပ်ရပါမယ်။ (အချို့ Methodology

တွေမှာ Forensics Image ကို ၂ ခုယူခိုင်းပါတယ်။ Analysis ပြုလုပ်နေရင်း တစ်ခုခုဖြစ်သွားရင် နောက်တစ်ခုနဲ့ အရန်သင့်ပြုလုပ်နိုင်အောင်ဖြစ်ပါတယ်။ Commercial Imaging Tools တွေမှာ Image စယူကတည်းက Forensics Image ၂ ခု တစ်ခါတည်းယူနိုင်ပါတယ်။) (ဒါတွေကို ရတဲ့အချိန်နဲ့ Image ယူတဲ့ Storage Size အပေါ်လဲမှုတည်ပြီး လုပ်ဆောင်နိုင်ပါတယ်။)

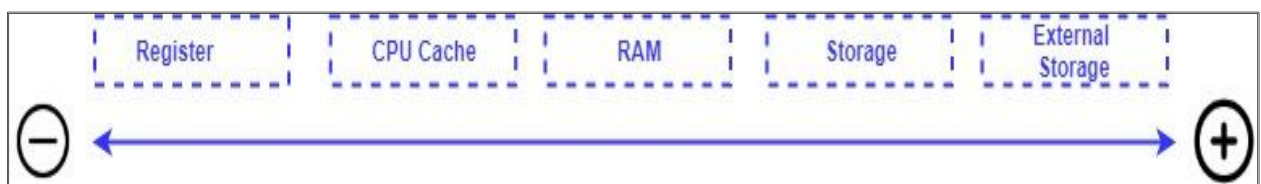
Volatility

Volatility ဆိုတာက Data တွေရဲ့ ပြောင်းလဲနိုင်မှု၊ သို့မဟုတ် Storage ပေါ်မှာ သိမ်းထားတဲ့ Data တွေ ဘယ်လိုအခြေအနေမှာ ပြောင်းလဲနိုင် ပျက်စီးနိုင်သလဲ ဆိုတာ ဖြစ်ပါတယ်။ ဥပမာ RAM ပေါ်မှာ သိမ်းထားတဲ့ Data တွေက Hard Disk ပေါ်မှာသိမ်းထားတဲ့ Data တွေထက်ပိုပြီး ပျက်စီးနိုင်ပါတယ်။ Restart/ Power Off တာနဲ့ RAM ပေါ်က Data တွေက Hard Disk မှာ သိမ်းထားတဲ့ Data တွေလိုမဟုတ်ပဲ ပျက်စီးသွားပါတယ်။

Order Of Volatility

Investigator တစ်ယောက်က Device ကနေ Evidence Acquire လုပ်တော့မယ်ဆိုရင် Order Of Volatility ကိုအရင်ဆုံးစဉ်းစားသင့်ပါတယ်။ အပေါ်က ဥပမာအတိုင်းပဲ RAM ပေါ်က Data တွေက Hard Disk မှာ သိမ်းထားတဲ့ Data တွေထက်ပိုပြီး ပျက်စီးနိုင်ပါတယ်။ ပုံတွင် Device ပေါ်မှာ Volatility ဖြစ်နိုင်မှု အနည်းအများအပေါ်မူတည်ပြီး ပြသထားပါတယ်။

CPU ထဲမက Register တွေက ပိုပြီး Assembly Instruction တွေကြောင့် ပျက်စီးမှု အများဆုံးဖြစ်နိုင်ပါတယ်။ ပျက်စီးနိုင်မှုအနည်းဆုံးက HDD and External Storage တွေပဲဖြစ်ပါတယ်။ Evidence Acquire ပြုလုပ်တဲ့အချိန်မှာ Order Of Volatility အတိုင်းဦးစား ပေးပြီး Acquire လုပ်သင့်ပါတယ်။ (Digital Forensics မှာတော့ RAM - Storage - External Storage စသည်ဖြင့် အစဉ်အတိုင်းသွားမှာ ဖြစ်ပါတယ်။)



Order Of Volatility

Type Of Data Acquisition

Data Acquisition နည်းလမ်းမှာ ၂ မျိုးရှိပါတယ်။

- Static Acquisition
- Dynamic / Live Acquisition

နည်းလမ်း 2 ခုထဲကမှ Order Of Volatility နဲ့ Case အပေါ်မူတည်ပြီး ဆောင်ရွက်ရမှာ ဖြစ်ပါတယ်။

Static Acquisition

Non – Volatile Data တွေကို Acquire လုပ်ခြင်း။ SystemReboot/Shutdown ဖြစ် သွားခဲ့ရင် မပျက်စီးပဲ ကျန်နေမဲ့ Data တွေကို Acquire ပြုလုပ်ခြင်းဖြစ်ပါတယ်။ ဥပမာ Hard-Disk, USB Stick စသည်ဖြင့် ဖြစ်ပါတယ်။

Dynamic / Live Acquisition

System Reboot/Shutdown ကျသွားရင် ပျက်စီးသွားနိုင်တဲ့ Data တွေကို System Live ဖြစ်နေတဲ့ အချိန်မှာ Acquire ပြုလုပ်တာ ဖြစ်ပါတယ်။ Live ဖြစ်နေတဲ့အချိန် ရရှိနိုင်မဲ့ Data တွေက ပိုပြီး အရေးကြီးတဲ့အချိန်မှာ ပြုလုပ်ခြင်းဖြစ်ပါတယ်။ ဥပမာ Incident Response ။ (Live ဖြစ်နေရင် ရနိုင်မဲ့ Data တွေ Bitlocker နဲ့ပတ်သတ်တာတွေကို Blog မှာရေးသားပြီး ဖြစ်ပါတယ်။)

ဒါပေမဲ့ Static Acquisition ပြုလုပ်တဲ့အခါမှာလဲ Dynamic / Live Acquisition မှာမရခဲ့တဲ့ Memory File တွေကို ရရှိနိုင်ပါတယ်။ (ဥပမာ။ Pagefile.sys hyperfil.sys) (ဒီအကြောင်းတွေကိုလဲ ရေးသားပြီး ဖြစ်ပါတယ်။)

Dead Acquisition

တစ်စုံတစ်ယောက်က Operation System မှာ Malwares/ Rootkits တွေကို Install ပြုလုပ်ထားတဲ့အချိန်မှာ Operation System က မယုံကြည်ရတဲ့အတွက် OS Dataတွေ မပါပဲ ကျန်တဲ့ Data တွေကို Acquire ပြုလုပ်ခြင်း ဖြစ်ပါတယ်။

Storage Formats

ကျွန်တော်တို့ Image ရယူမည့် အချိန်မှာ စဉ်းစားရမဲ့ အချက်က ကိုယ်ယူမဲ့ Forensics Image က ဘယ်လို Image File Type မျိုးနဲ့ရယူရမလဲ Forensics Image ကိုဘယ်နေရာမှာ သိမ်းမလဲဆိုတာပဲ ဖြစ်ပါတယ်။ အသုံးပြုတဲ့ Imaging Tools အပေါ်မူတည်ပြီး Forensics Image ကို Read, Write, Analysis ပြုလုပ်တာ မှာ ကွာခြားနိုင်ပါတယ်။

Raw Format

Forensics Image ပြုလုပ်တဲ့နေရာမှာ လွယ်ကူရိုးရှင်းတဲ့နည်းလမ်းဖြစ်ပါတယ်။ RAW ဆိုတာက The data is read from the source device's disk written on the file ဖြစ်ပါတယ်။ Raw Format ပြုလုပ်ပြီး Mount and analysis ပြုလုပ်တာကို နောက်ပိုင်းမှ ပြုလုပ်နိုင်ပါတယ်။

Raw Format က Data Transfer Rate မြန်ဆန်သလို Forensics Tools တော်တော် များများမှာလဲ အသုံးပြုနိုင်ပါတယ်။ မတူညီတဲ့ Forensics Tools တွေနဲ့ တွဲဖက်အသုံးပြုနိုင်ပြီး ရလာတဲ့ Result ကို Cross Check လုပ်လို့လွယ်ကူပါတယ်။ (ဥပမာ Encase မှာ Raw Format ကို ထည့်သွင်းပြီး Analysis ရလာတဲ့ Result နဲ့ Autopsy မှာ Raw Format ကို ထည့်သွင်း ပြီးရလာတဲ့ Result ကို နှိုင်းယှဉ်ကြည့်ခြင်း။)

အားနည်းချက်ကတော့ Raw Format က Data Read တဲ့နေရာမှာ Disk ပေါ်က Error အချို့ကို မဖော်ပြ မပြင်ဆင်ပါဘူး။ ဒါကတော့ ကောင်းတာနဲ့ဆိုးတာကို စဉ်းစားရမဲ့ အချက်ပါ။ နောက်တစ်ခုက Image File သိမ်းဖို့ နေရာလုံလောက်မှုရှိဖို့ပါ။ Disk က 100 GB ဆိုရင် Forensics Image ကလဲ 100 GB ဖြစ်မှာပါ။ Imaging ပြုလုပ်တဲ့အခါမှာ Forensics Image File ကို Handle လုပ်ရတာလွယ်အောင် ခွဲထုတ်တာ လုပ်လို့ရပါတယ်။ ဥပမာ 100 GB ရှိတဲ့ Image File မလုပ်ပဲ 10 GB ရှိတဲ့ Image File 10 ခု ခွဲထုတ်တာမျိုးပါ။

Raw Format ပြုလုပ်တဲ့နေရာမှာ Open Source ဖြစ်ပြီး နာမည်ကြီးတဲ့ Tools ကတော့ DD Tool ပဲ ဖြစ်ပါတယ်။ Image File ရော Image File ကို ခွဲထုတ်တာတွေပါ ပြုလုပ်လို့ရပါတယ်။ Linux မှာ built-in ပါဝင်ပါတယ်။ Window အတွက်ဆိုရင်တော့ Raw Write Studio ဖြစ်ပါတယ်။

DD Tools အသုံးပြုပုံက ရိုးရှင်းပါတယ်။

dd if = [Source Device] of=[Destination]

dd if=/dev/sda of=/share/image.img

dd if = [Source Device] | split -b <Split Size> - <File Name>

dd if=/dev/sda | split -b 1000m - image.img

DD မှာ တစ်ခုရှိတာက အခြား Imaging Tools တွေလို Imaging လုပ်တဲ့ အချက်အလက် များဖြစ်တဲ့ headers, metadata စတဲ့ အချက်အလက်တွေမပါပါဘူး။ Bad Sector တွေကိုလဲ မဖတ်နိုင်ပါဘူး။

Proprietary Tools

Commercial Tools တော်တော်များများမှာတော့ Imaging ပြုလုပ်တာကို သူတို့ရဲ့ ကိုယ်ပိုင် Format နဲ့ ပြုလုပ်ပါတယ်။ ရလာတဲ့ Forensics Image Format ကိုလဲ သူတို့ရဲ့ကိုယ်ပိုင် Analysis Tool နဲ့သာ Analysis ပြုလုပ်လို့ရပါတယ်။ အခုတော်တော် များများမှာတော့ Cross Platform အသုံးပြုလို့ရနေပါပြီ။

Commercial Tools တွေက Forensics Image က Raw Format ထက်ပိုပြီး ပြည့်စုံကောင်းမွန်ပါတယ်။ Imaging and Analysis ပြုလုပ်ရာမှာ နှေးပေးမဲ့ Result အပိုင်းမှာ ပိုမိုကောင်းမွန်ပါတယ်။

Proprietary တွေရဲ့အားသာချက်ကတော့

- Space သိပ်မယူပါဘူး။
- Case နဲ့ပတ်သတ်တဲ့ Metadata တွေပါဝင်ပါတယ်။
- Single File အနေနဲ့ Data တွေကို သိမ်းဆည်းပါတယ်။

(Case Number. Device Name . etc ..)

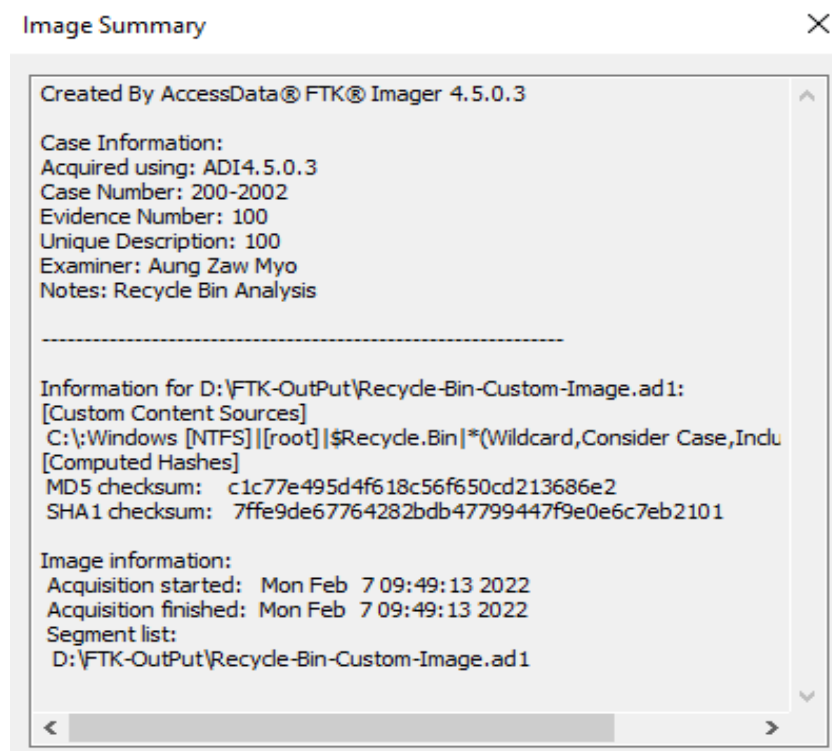
- Commercial Tools တွေမှာ အပြည့်အစုံပါဝင်တာကြောင့် Inverstigator ကနေ တစ်နေရာထဲမှာ Imaging, Analysis, Report လုပ်တာတွေပြုလုပ် လို့ရပါတယ်။

Proprietary တွေရဲ့အားနည်းချက်တွေကတော့

- ❖ Compression, Decompression, Encoding, Decoding Process ကြောင့် နှေးကွေးပါတယ်။

Commercial Forensics Image Examples

Encase image formats (E01 or Expert Witness Files (EWF), SMART, and AD1) and Access Data Image Formats (.AD1)



Example Forensics Image Note


```
Recycle-Bin-Custom-Image.ad1.txt - Notepad
File Edit Format View Help
Created By AccessData® FTK® Imager 4.5.0.3

Case Information:
Acquired using: ADI4.5.0.3
Case Number: 200-2002
Evidence Number: 100
Unique Description: 100
Examiner: Aung Zaw Myo
Notes: Recycle Bin Analysis

-----

Information for D:\FTK-OutPut\Recycle-Bin-Custom-Image.ad1:
[Custom Content Sources]
C:\:Windows [NTFS][[root]]$Recycle.Bin|*(Wildcard,Consider Case,Include Subdirectories)
[Computed Hashes]
MD5 checksum: c1c77e495d4f618c56f650cd213686e2
SHA1 checksum: 7ffe9de67764282bdb47799447f9e0e6c7eb2101

Image information:
Acquisition started: Mon Feb 7 09:49:13 2022
Acquisition finished: Mon Feb 7 09:49:13 2022
Segment list:
D:\FTK-OutPut\Recycle-Bin-Custom-Image.ad1
```

Example Forensics Image Note

Advanced Forensics Format (AFF)

Advanced Forensics Format (AFF) က Basic Technology (Auopsy) ကနေပြုလုပ်ထားတဲ့ Open Source Forensics Image တစ်ခုဖြစ်ပါတယ်။ Disk Space သက်သာပြီး Investigator က Custom Field တွေ အပ်လို့ရပါတယ်။ Image or Separate file တွေမှာ metadata တွေ အပ်လို့ရပါတယ်။ AFF ကို Open Source နဲ့ အခြား Commercial Tools တွေမှာပါ Support ပေးပါတယ်။ AFF က Device Storage ကနေ 16 MB ရှိတဲ့ Block (Page) တွေကို Copy ပြုလုပ်တာဖြစ်ပါတယ်။ (SSD အတွက်အဓိကထားပြီး အသုံးပြုပါတယ်။)

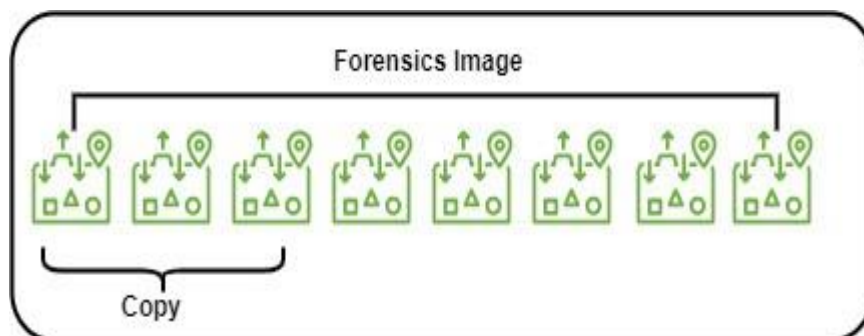
အရင်က AFF Version အဟောင်းတွေမှာ ပြဿနာ နည်းနည်းရှိပါတယ်။ Live ဖြစ်နေတဲ့ Data တွေကို Collect ပြုလုပ်လို့မရခြင်း Encryption မပါဝင်ခြင်း၊ 16 MB Page Size ကြောင့် NTFS Metadata တွေကို Collect ပြုလုပ်လို့မရခြင်းတို့ဖြစ်ပါတယ်။ နောက်ပိုင်း Version တွေမှာ ဒီလိုပြဿနာတွေမရှိတော့ပါ။

Data Acquisition And Copy

Data Acquisition ပြုလုပ်တယ်ဆိုတာ Copy ပြုလုပ်တာမဟုတ်ပါဘူး။ အဓိကကွဲပြားခြားနားချက်တွေက

- ✓ Imaging – Device Storage တစ်ခုလုံးကို File အဖြစ်ပြုလုပ်တာဖြစ်ပါတယ်။
- ✓ Copying – အသုံးဝင်မဲ့ Data အချို့ကိုပဲ Source Device ကနေ ကူးယူတာဖြစ်ပါတယ်။

ဥပမာ - တစ်ကယ်လို Hard Disk တစ်လုံးမှာ 100 ရာနှုန်းရှိခဲ့ရင် 60 ရာနှုန်းကိုပဲ အသုံးပြုနေတာဖြစ်ပြီး ကျန်တဲ့ 40 ရာနှုန်းက Delete File , Random Bytes, Unused Part တွေပဲဖြစ်ပါတယ်။ Imaging ပြုလုပ်တာက Storage တစ်ခုလုံးမှာရှိတဲ့ အသုံးပြုတဲ့ အပိုင်းရော အသုံးမပြုတဲ့ အပိုင်းကိုရော ပြုလုပ်တာဖြစ်ပါတယ်။ Copying ပြုလုပ်တာက အသုံးပြုထားတဲ့ Storage ရဲ့ 60 ရာနှုန်းကိုသာ ကူးယူတာဖြစ်ပါတယ်။



Data Acquisition & Copy

Acquisition Issues

- ❖ အပေါ်မှာ ပြောခဲ့သလိုပဲ မူရင်း System/Storage နှင့်တိုက်ရိုက် Analysis မပြုလုပ်ရန်။
- ❖ မူရင်း System/Storage ကို Image ရယူပြီး လုံခြုံစွာသိမ်းဆည်းရန်။

- ❖ Chain Of Custody ကို အထောက်အကူဖြစ်စေရန် နှင့် Investigator မှ လိုအပ်သလောက်သာ Forensics Image ပြုလုပ်ရန်။

Investigator မှ Forensics Image ပြုလုပ်နေစဉ် စဉ်းစားရန်လိုအပ်သည့်အချက်အလက်များ

Forensics Image ပြုလုပ်ရာတွင် Image File သည် မူရင်း Storage Size နှင့် ထပ်တူကျရာမှာ ဖြစ်ပါတယ်။

- မူရင်း System/Storage ကို Image ပြုလုပ်ပြီး System/Storage အပေါ်ကို ပြောင်းလဲပြင်ဆင်မှု မပြုလုပ်မီစေရန် သတိထားရမည်။ မဟုတ်လျှင် Analysis Results နှင့် မကိုက်ညီခဲ့လျှင် Authentic ဖြစ်မည်မဟုတ်ပါ။
- System/Storage ပြုလုပ်နေစဉ် မူရင်း System/Storage မပျက်စီး၊ အတွင်းမှ အချက်အလက်တွေ မပြောင်းလဲစေရန် သတိထားရမည်။

Acquisition Methods

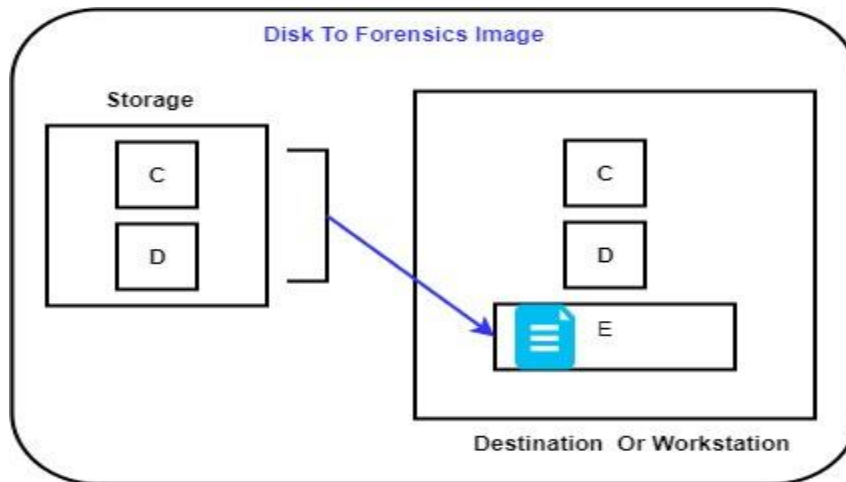
Data Acquisition ပြုလုပ်ရာတွင် နည်းလမ်း 2 မျိုးရှိပါသည်။ နည်းလမ်းတစ်ခုနှင့်တစ်ခုတွင် Output မတူညီပါ။

- ✓ Disk Drive To Image File (Imaging)
- ✓ Disk Drive To Disk Drive (Cloning)

Disk Drive To Image File (Imaging)

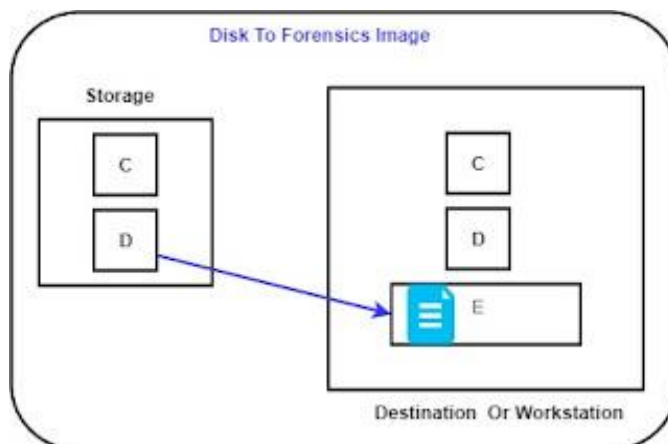
Disk Drive To Image File (Imaging) သည် System/Storage တစ်ခုလုံးအား Image File အဖြစ်သို့ပြောင်းလဲခြင်းဖြစ်ပါသည်။ Drive Imaging ပြုလုပ်တာကို Forensics

Image ပြုလုပ်တယ်လို့လဲ ခေါ်ဆိုပါတယ်။ Disk Drive To Image File (Imaging) ပြုလုပ်တဲ့ နည်းလမ်းက Scalability, Efficiency ပိုဖြစ်ပါတယ်။ Investigator မှ လိုအပ်သလောက် Forensics Image ပြုလုပ်နိုင်ပြီး Image File ကို သိမ်းဖို့ နေရာရှိဖို့ပဲ လိုအပ်ပါတယ်။



Disk To Forensics Image

Forensics Image ပြုလုပ်ရာမှာ Full Disk တစ်ခုလုံးပြုလုပ်သင့်တယ်လို့မဆိုလိုပါ။ Storage တစ်ခုမှာ Partition တစ်ခုထက်ပိုပြီးရှိနိုင်ပါတယ်။ Case လိုလားချက် နှင့် Investigator ဆုံးဖြတ်ချက်အပေါ်မူတည်ပြီး Full Disk သို့မဟုတ် Partition တစ်ခု သို့မဟုတ် နှစ်ခု ကို Forensics Image ရယူနိုင်ပါတယ်။ မိမိ အခြေအနေ လိုလားချက် Anlysis ပြုလုပ်မဲ့ အပေါ် မူတည်ပြီး (Imaging) ဒါမှမဟုတ် Disk (Cloning) ရယူဖို့ရွေးချယ်ရမှာဖြစ်ပါတယ်။

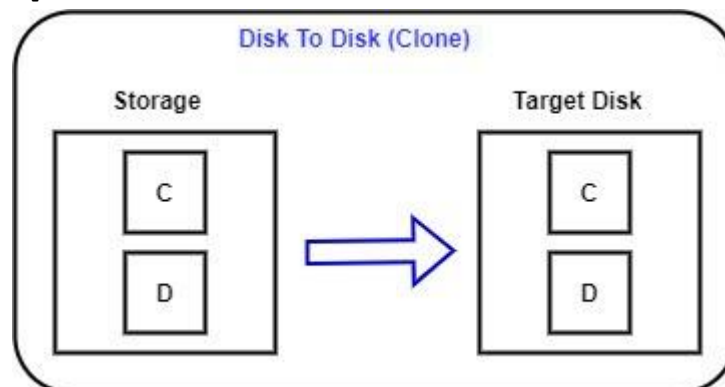


Disk To Forensics Image

အရေးကြီးတဲ့အချက်ကတော့ Evidence နဲ့ပတ်သတ်လာရင် Forensics Image ပြုလုပ်ပြီးမှ investigation ပြုလုပ်ရန်ဖြစ်ပါတယ်။ Forensics Image တစ်ခုထဲ မပြုလုပ်မီပါစေနဲ့ Analysis ပြုလုပ်နေစဉ်မှာ Error တွေ Corrupt ဖြစ်တာတွေရှိလာ နိုင်တဲ့အတွက်ဖြစ်ပါတယ်။ နောက်ဆုံး သတိပေးချင်တာက Forensics Image သိမ်းဆည်း တဲ့နေရာက ဘယ်နေရာမဆို သိမ်းဆည်းနိုင်ပေမဲ့ Same Disk ပေါ်ကို မသိမ်းမိစေ ဖို့ဖြစ်ပါတယ်။ Evidence သိမ်းဖို့ သီးခြား Storage သို့မဟုတ် SAN ပေါ်မှာ သိမ်းဆည်း သင့်ပါတယ်။

Disk Drive To Disk Drive (Cloning)

Disk Drive To Disk Drive (Cloning) ပြုလုပ်တာကတော့ မူရင်း Storage နဲ့ ပမာဏတူတဲ့ အခြား Storage ပေါ်ကို Data တွေကို Acquisition ပြုလုပ်တာဖြစ်ပါတယ်။ Clone ပြုလုပ်တယ်လို့လဲ ခေါ်ပါတယ်။



Disk To Disk (Clone)

Spare Acquisition

Spare Acquisition က Investigator က Storage တစ်ခုလုံးကို ကူးယူတာမဟုတ်ပဲ လိုအပ်တယ် သံသယရှိတယ်ဆိုတဲ့ အပိုင်းကိုပဲ ကူးယူတာဖြစ်ပါတယ်။ Spare Acquisition က Down Time ပေးလိုမရတဲ့နေရာတွေ Storage ပမာဏ အရမ်းများနေတဲ့အတွက် Forensics Image မပြုလုပ်နိုင်တဲ့အချိန်တွေ၊ အရေးတကြီး Result လိုနေတဲ့အချိန်တွေမှာ

ပြုလုပ်နိုင်ပါတယ်။ Spare Acquisition မှာ တစ်ခုရှိတာက Investigator မှ ဘာကိုပဲ Forensics Image ရယူမယ်ဆိုတာ သေချာစွာ သိရှိနေဖို့ဖြစ်ပါတယ်။

ဥပမာ - Unallocated Space Only, Web Server Logs, FTP Server Log, Recent Log, Etc

Choosing Acquisition Method

အခုလောက်ဆိုရင် ဘယ်လို Acquisition Method ကို သုံးစွဲဖို့ ရွေးချယ်ရမလဲ ဆိုတာသိလောက်ပြီ ဖြစ်ပါတယ်။ Acquisition Method တစ်ခုပဲ အမြဲတမ်းမှန်တယ် သုံးစွဲရမယ်လို့မရှိပါဘူး။ Case တိုင်းမှာ မတူညီတဲ့ အခြေအနေတွေရှိတာကြောင့် မတူညီတဲ့ Methods တွေကို အသုံးပြုနေ လိုအပ်နေမှာ ဖြစ်ပါတယ်။

Acquisition Methods

Disk and Image

Forensics Image ကိုအသုံးပြုတာကတော့ Image ကို သိမ်းထားဖို့နေရာရှိရင် အသုံးပြုလို့ ပိုပြီးကောင်း ပါတယ်။ ဒါပေမဲ့ Image ပြုလုပ်နေစဉ် Bug သို့မဟုတ် Error တွေရှိတတ်တာကြောင့် Forensics Image ကိုအမြဲတမ်းအသုံးပြုလို့မရနိုင်ပါဘူး။ ဒါကြောင့် Disk To Disk Clone Method ကို အသုံးပြုသင့်ရင် အသုံးပြုရပါလိမ့်မယ်။

Spare and Logical Disk

Spare Acquisition , Logical Disk Acquisition နည်းလမ်း ၂ ခုစလုံးက အချိန်အကန့် အသတ်ရှိတဲ့ အခါမျိုးမှာဆိုရင် အသုံးပြုဖို့ အသင့်တော်ဆုံး နည်းလမ်း ဖြစ်ပါတယ်။ Spare Acquisition က Logical Disk Acquisition နည်းလမ်းထက်ပိုပြီး မြန်ဆန်ပါတယ်။ ကိုယ်သိမ်းချင်တဲ့ File က Acquire လုပ်တဲ့ Tools မှာ အဆင်သင့် မပါလာရင် Collect လုပ်လို့မရပါဘူး။ Manual သတ်မှတ်ပေးရပါမယ်။ ပြီးရင် ကိုယ်က ဘယ်နေရာက File ကိုရယူရမယ်ဆိုတာ သိထားမှ အဆင်ပြေမှာ ဖြစ်ပါတယ်။ Logical Disk Acquisition နည်းလမ်းကတော့ Spare Acquisition နည်းလမ်းထက်ပိုပြီး အချိန်ယူပါတယ်။ Logical Disk Size အပေါ်မူတည်ပြီး Acquisition လုပ်ရမှာ ဖြစ်ပါတယ်။

Live Acquisition

Live Acquisition ပြုလုပ်တာကို System Run နေစဉ်ပြုလုပ်ရမှာဖြစ်ကြောင်း အရင်ကပြောခဲ့ပြီးဖြစ်ပါတယ်။ Live Acquisition ပြုလုပ်နေစဉ် Investigator က Volatile Data ကိုအရင်ဆုံးရယူရမှာ ဖြစ်ပါတယ်။ Volatile Data က Memory ထဲမှာရှိတာကြောင့် System Reboot/Shutdown ဖြစ်တာနဲ့ ပျောက်သွားမှာ ဖြစ်ပါတယ်။ Volatile Data တွေက အမြဲတမ်း RAM, Cache ထဲမှာရှိပါတယ်။ Volatile Data က System Reboot/Shutdown ကြောင့်ပျောက်ကွယ်နိုင်ရုံတင်မက Modification, Alteration ဖြစ်တတ်ပါတယ်။ ဘာလို့လဲဆိုရင် System ပေါ်မှာ Run နေတဲ့ Process မှန်သမျှက Ram, Cache တွေကို အမြဲတမ်း သုံးနေရတာကြောင့်ဖြစ်ပါတယ်။ System ပေါ်မှာ လှုပ်ရှားတာမှန်သမျှ လုပ်ကိုင်တာမှန်သမျှက RAM ပေါ်ကိုသွားပြီး သက်ရောက်မှာ ဖြစ်ပါတယ်။

Volatile Data တွေက အချိန်တိုအတွင်း ပျက်စီးလွယ်ပေမဲ့ Process တွေက RAM ကိုအသုံးပြုပြီး Run တာဖြစ်တဲ့အတွက် Password, Messages, IP address စတာတွေကို ရရှိနိုင်ပါတယ်။ ဒါကြောင့် Malwares Analysis /Hunting တွေမှာပါ အသုံးပြုနိုင်ပါတယ်။

Memory ပေါ်မှ ရရှိတဲ့ Encryption Key က Malwares နဲ့ သူရဲ Operator ကြားက Traffic ကို Extract, Decrypt လုပ်နိုင်ပါတယ်။ Volatile Data အားလုံးက RAM ပေါ်မှာရှိတယ်လို့ပြောမယ်ဆိုရင် မှားပါလိမ့်မယ်။ Non-Volatile ဖြစ်တဲ့ Storage ပေါ်မှာလဲ ရှိပါတယ်။ ဥပမာ Temporary File, Log File

Log File တွေကတော့ အချိန်ကာလတစ်ခုအတွင်းမှာ Log Rotate ကြောင့် ပျက်စီးနိုင်သလို၊ Temporary File တွေက တစ်ခါတစ်ရံ Automatic ပျက်စီး နိုင်ပါတယ်။

SYS Info ဆိုတာက Basic System Information ဖြစ်တဲ့ System အကြောင်း၊ OS အကြောင်း ၊ Installed Application တွေအကြောင်းကိုဖော်ပြတာဖြစ်ပါတယ်။ OS Version, OS Configuration, OS Build Number, Product Key Computer Name, User Account, Manufacture and specs (CPU model, RAM size, etc) စတာတွေကိုပါ ဖော်ပြပါတယ်။

OS Configuration က Collect လုပ်ရာမှာလဲ အရေးကြီးတဲ့နေရာ ကနေပါဝင်ပါတယ်။ OS Configuration ဖြစ်တဲ့ Installed Languages, System Up Time, Time Zone, Install Update စတာတွေကို Collect လုပ်သင့်ပါတယ်။ ဒါမှသာ စစ်ဆေးသူက OS

အကြောင်း နဲ့ File 2 ခုရှိရင် ဘယ်ကနေလဲတာလဲ ကွန်ပျူတာ အတူတူကနေ လာတာလား ဒါမှမဟုတ် အခြားနေရာကနေ လာတာလား ဆိုတာကို သိရမှာ ဖြစ်ပါတယ်။

Live Acquisition လုပ်နေစဉ်မှာ System မှာ ဘယ်လို Process တွေ Running လုပ်နေတာဆိုတာကို သိထားခြင်းက Investigation အတွက် အရေးပါပါတယ်။နောက်ထပ် ဘာတွေထပ်ပြီး Acquisition လုပ်ရမယ်။ စစ်ဆေးသူက RAM Dump ကို Analysis လုပ်ချိန်မှာ ဘာကို စစ်ဆေးရမယ်ဆိုတာကို သိဖို့ အထောက်အကူပြုပါတယ်။

တစ်ခါတစ်ရံ Investigation Analysis ပြုလုပ်နေချိန်မှာ log ရှာတာနဲ့တင် အချိန် အတော်ကြာပါတယ်။ Log Details ရရင် Investigator က Incident Timeline ဆောက်တဲ့ အချိန်မှာ အသုံးဝင်ပါတယ်။ Incident Response မှာ ဖြစ်တဲ့ အချိန်မတိုင်ခင် ဘယ်လို တွေ့ကြောင့် ဖြစ်တာလဲဆိုတာ စစ်ဆေးရပါတယ်။

Main Log ရယ်လို့မရှိပဲ System မှာသုံးထားတဲ့ Applications, လုပ်ဆောင်မှု အပေါ်မူတည်ပြီး log တွေရှိပါတယ်။ OS Event Logs, Process Log, Network Log စသည်ဖြင့်အမျိုးမျိုးရှိနိုင်ပါတယ်။ Time Stamp ကလဲ Crime Reconstruction အပိုင်းမှာ အဓိက ကျတဲ့နေရာကနေပါဝင်ပါတယ်။ ဒါကို Timeline Analysis လို့ခေါ်ပြီး အချိန်တစ် ခုအတွင်းမှာ ဖြစ်ပျက်ခဲ့တာတော်ကိုသိနိုင်ဖို့ ဆက်နွှယ်နေတဲ့ Event Log တွေကိုရှာဖွေ ပါတယ်။

Network Configuration ကလဲ အရေးကြီးပါတယ်။ အထူးသဖြင့် Network Attack ဝင်လာတဲ့ အချိန်မျိုးတွေမှာ ဖြစ်ပါတယ်။ NIC card, Mac Address, IP Address စတာတွေက Analysis လုပ်နေချိန်မှာ Investigator ကို အထောက်အကူပြုနိုင်ပါတယ်။

Memory Forensics က အခြား Filesystem, Operation System, Network Protocol လိုမျိုး တွဲဖက်စစ်ဆေးစရာ စက်ပစ္စည်း မရှိတဲ့ အတွက် ပြုလုပ်ရတာ မလွယ်ကူပါဘူး။ File, OS, Network တွေကို Analysis လုပ်တဲ့အခါမှာ Case အတွက်လိုအပ်တဲ့ အချက်အလက်တွေ မရတာမျိုးတွေကြုံရတတ်ပါတယ်။ Full Disk Encryption လိုမျိုးဆိုရင် Suspect ဆီကနေ Encryption Key မရရင်ခွဲရင် Memory Forensics ပြုလုပ်တဲ့နည်းလမ်းပဲ ရှိပါတယ်။ (Bitlocker , TPM , VeraCrypt တို့အကြောင်းရေးသားပြီး ဖြစ်ပါတယ်။)။ အခုခေတ်မှာ Data လုံခြုံရေး အတွက် Security Solution တွေအများကြီးရှိနေပြီ။ ဒါကြောင့် Forensics Image ပြုလုပ်ဖို့မလွယ်ကူတော့ပါ။

Advanced Persistent Threat, Malware, Rootkit တွေရဲ့ Track ကို စစ်ဆေးဖို့အတွက်လဲ Memory Forensics ကိုပြုလုပ်ပါတယ်။အချို့သော Malwares တွေက ခြေရာဖျောက်ဖို့ RAM ထဲမှာပဲရှိနေပြီး Storage ပေါ်မှာ အလုပ်မလုပ်ပါဘူး။ ဒါကြောင့် Memory Forensics ပြုလုပ်ရတာဖြစ်ပါတယ်။ Network Packet Content, Browsing History, Injected Code (Malwares, BOF Attack), Process Data, Clipboard Data တွေက Memory ထဲကနေရရှိနိုင်ပါတယ်။

Live Acquisition Or Live Response အတွက် Memory Image ရယူဖို့ Analysis လုပ်ဖို့ အတွက် Tools တွေအများကြီးရှိပါတယ်။ အချို့သော Tools တွေက Personal Information ဖြစ်တဲ့ Credit Card Number, Phone Numbers တွေကိုရှာပေးပြီး အချို့ကတော့ Email, Chat, CMD Command စတာတွေကို ရှာဖွေပေးပါတယ်။

ဥပမာ RAM Acquisition အတွက် GUI Tools ဖြစ်တဲ့ FTK Imager, Belkasoft RAM Capture. Analysis အတွက် Volatility

Tools

Acquisition လုပ်နေတဲ့ အချိန်မှာ အချို့သော ပြဿနာတွေကို ရှင်းလင်းဖို့ Tools တွေ Utilities တွေရှိပါတယ်။ အပေါ်မှာပြောခဲ့သလိုပဲ Acquisition စလုပ်တဲ့ အချိန်မှာ Original Storage Media ကို မသမာမှုတစ်ခုခု သို့မဟုတ် အမှားအယွင်းတစ်ခုခုလုပ်မိလို့ စတာတွေကြောင့် Investigation Process ပျက်စီးနိုင်ပါတယ်။ Evidence Integrity ပျက်စီးနိုင်တယ်လို့ဆိုလိုတာပါ။

Write Blocker က Acquisition ပြုလုပ်စဉ်မှာ Evidence Integrity မပျက်စီးအောင် ပြုပြင်ပြောင်းလဲလို့မရအောင် Investigator ကိုကူညီပေးပါတယ်။ Write Blocker က Storage ပေါ်ကို Data တွေထပ်ပြီးထည့်လို့မရ Write မလုပ်နိုင်အောင် လုပ်ပေးပါတယ်။Write Blocker တွေက Hardware Software မျိုးစုံရှိပါတယ်။ ရိုးရိုး Write Blocker တွေတင်မက အခု Imaging နဲ့ Write Protect Function ပါတဲ့ Hardware တွေပေါ်နေပါပြီ။

Bootable Disks ကိုတော့ Suspect ရဲ့ Computer ရဲ့ Main Storage ကိုမထိပဲ Storage Acquisition Or RAM Acquisition ပြုလုပ်တဲ့ အချိန်မှာ အသုံးပြုပါတယ်။ ဥပမာ Paladin Boot, Kali Forensics Mode, Etc.

Non Writeable USB

Investigator က Bootable USB Disk နဲ့ Acquisition လုပ်ချိန်မှာ Data Export လုပ်ဖို့အတွက် USB , External HardDisk တွေကိုသုံးရတာရှိပါတယ်။ Evidence ပါတဲ့ Storage ကို Workstation မှာထိုးတဲ့အခါ အခန့်မသင့်ရင် Evidence Integrity ပျက်စီးနိုင်ပါတယ်။ အဲဒီလိုအခါမျိုးမှာ Write Bocker ကို အသုံးပြုသင့်ပါတယ်။

ဒါပေမဲ့ Writ Blocker အသုံးပြုဖို့ ဥပဒေမရှိတဲ့ နိုင်ငံတွေလဲ ရှိပါသေးတယ်။အသုံးပြုဖို့ အဆင်မပြေတဲ့အခါမျိုးတွေမှာ Workstation ရဲ့ Window မှာ Write Blocking ကို လွယ်လွယ်ကူကူပြုလုပ်လို့ရပါတယ်။ Window Registry ကနေပြုလုပ်ရမှာဖြစ်ပြီး Write Access မှန်သမျှကို Block ပြုလုပ်ပေးမှာဖြစ်ပါတယ်။ အောက်ကပုံတော့ Write Blocker နဲ့ Imager ကိုပေါင်းထားတဲ့ Hardware Device ဖြစ်ပါတယ်။

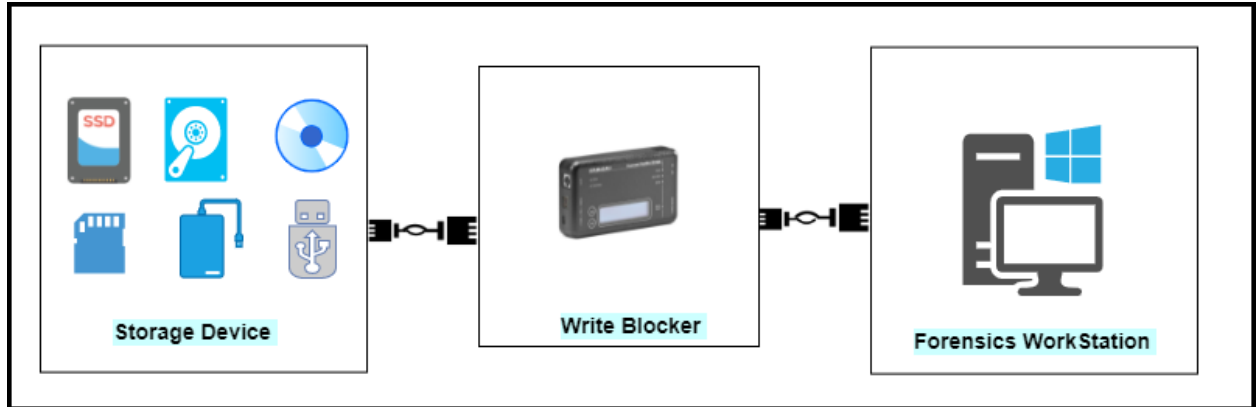


Imager + Write Blocker

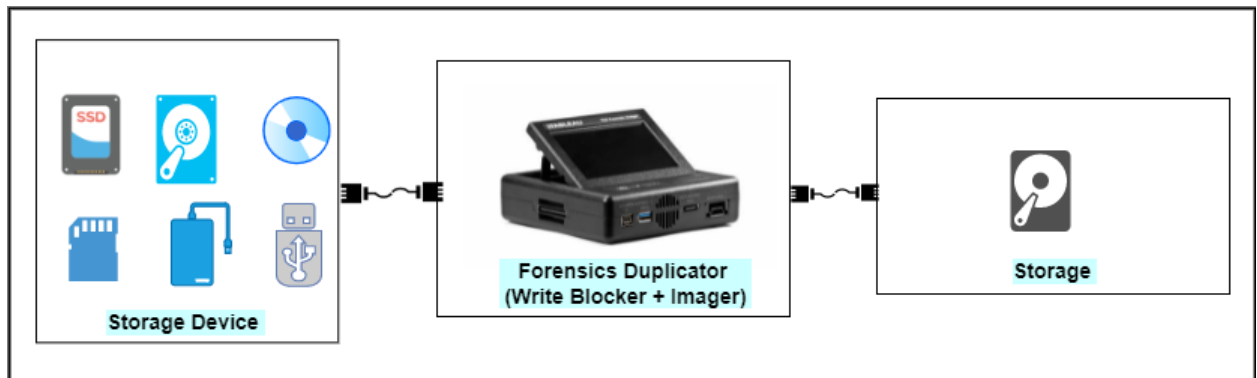


Write Blocker Only

အောက်ဖော်ပြပါပုံတွေကတော့ Imaging Process ကို မျက်စိထဲမြင်သာအောင် ပြသထားတာ ဖြစ်ပါတယ်။ Write Blocker အသုံးပြုတာမပြုတာကတော့ သက်ဆိုင်ရာ နိုင်ငံတွေရဲ့ ဥပဒေပေါ်မှာလဲမူတည်ပါတယ်။ Write Blocker တွေက ဈေးကြီး တဲ့အတွက် Computer မှာလဲ Registry ကနေ Write Protect ပြုလုပ်နိုင်ပါတယ်။



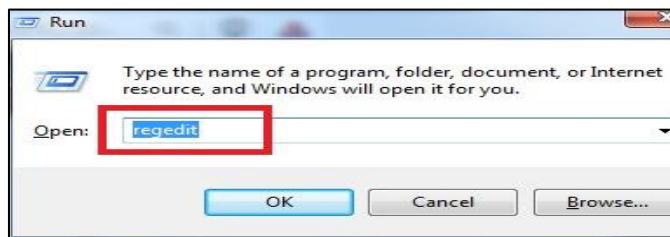
Write Blocker Only Diagram



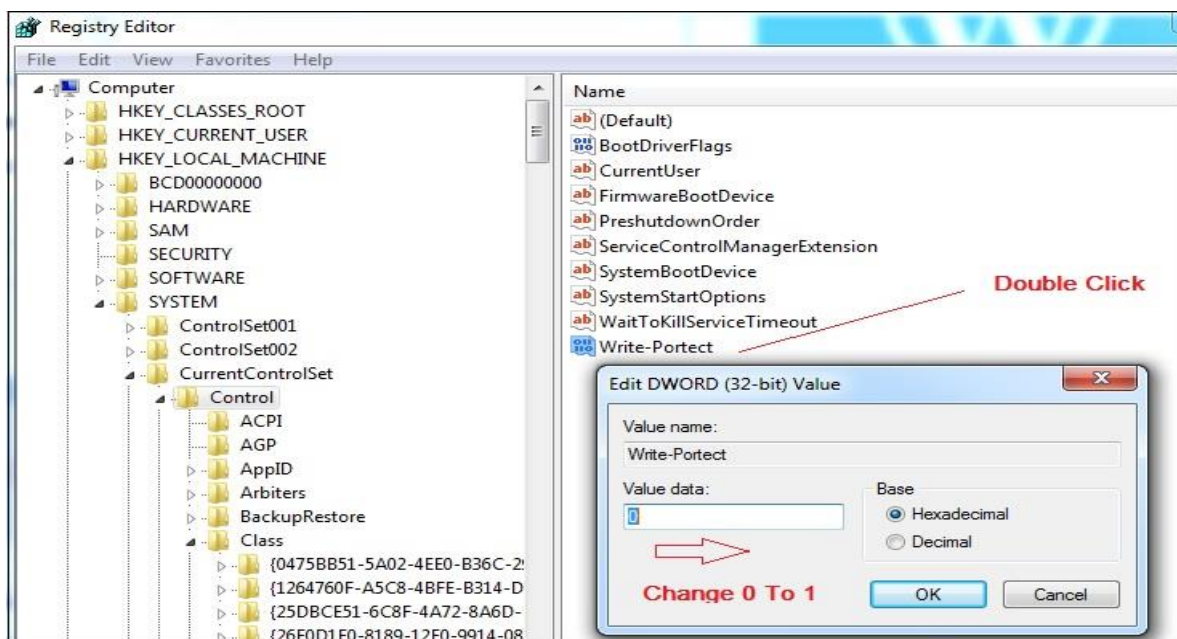
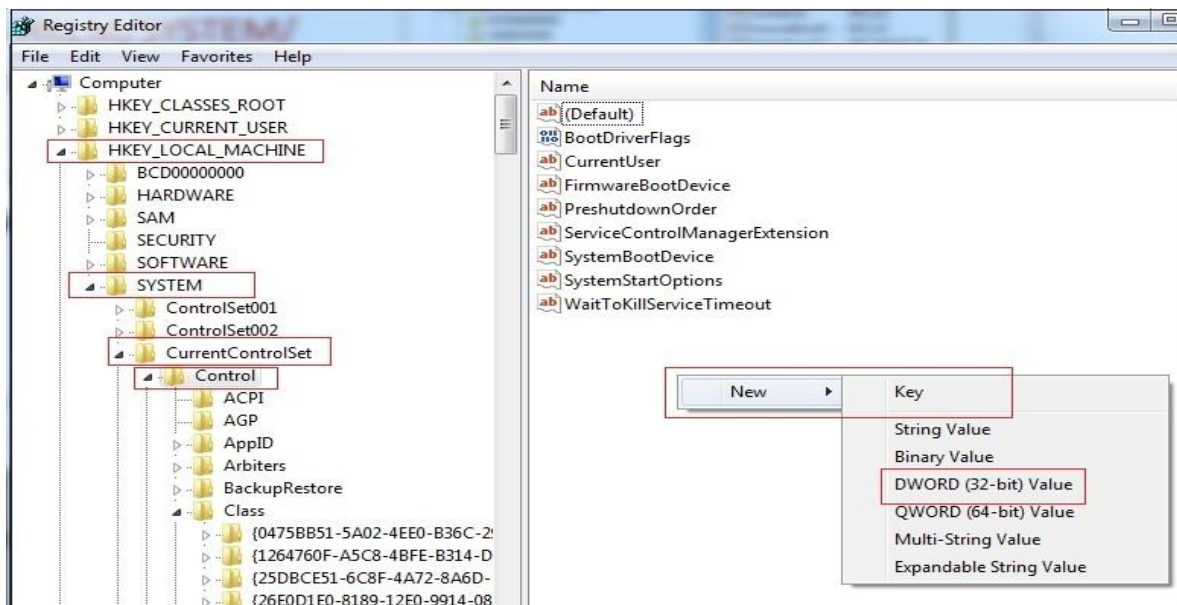
Imager + Write Blocker Diagram

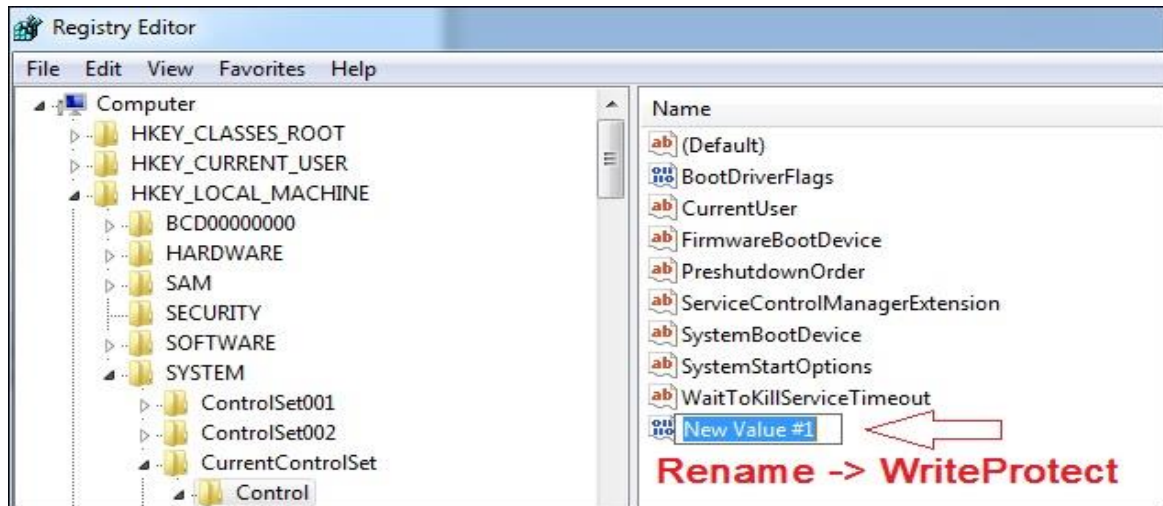
Write Protect In Registry

Microsoft က Windows XP မှစပြီး USB Write Protect ကို ပြုလုပ်လို့ရပါတယ်။ Write Blocker တွေက ဈေးကြီး တဲ့အတွက် USB Write Protect ကို Work Station မှာ ပြုလုပ်နိုင်ပါတယ်။ HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control ထဲမှာ New Key Storage Device Policies ကို ပြုလုပ်ရမှာ ဖြစ်ပါတယ်။ Write Protect ကို disable ပြန်လုပ်ချင်ရင် 1-0 ပြန်ပြောင်းပေးရမှာ ဖြစ်ပါတယ်။ Window +R ---- > (Regedit)



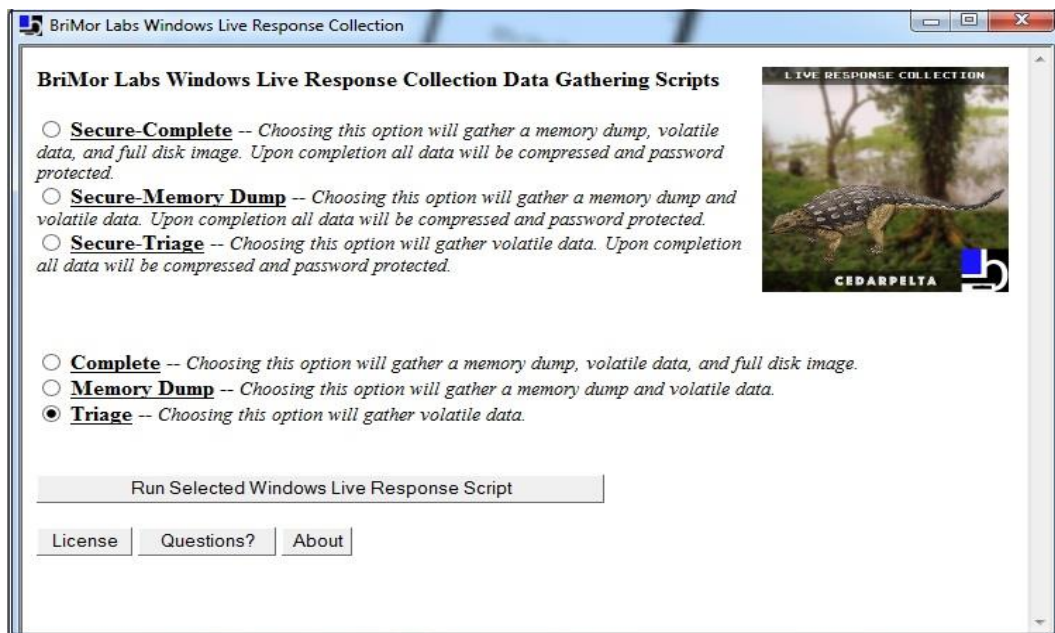
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control





Live Response

Live Response အတွက် eCDFP က ညွှန်းထားတာကတော့ brimorlabs ပဲဖြစ်ပါတယ်။ Live Response အတွက် Linux, Window, Mac အတွက် အစုံပါပါတယ်။ Result File တွေက brimorlabs ရှိတဲ့ Folder ထဲသွားသိမ်းမှာ ဖြစ်ပါတယ်။ Download [BriMor Labs - Tools](#)



Main Page

```
Administrator: Live Response Collection (Cedarpelta Build - 20190905)

C:\Users\AungZawMyo\Downloads\Compressed\Windows_Live_Response>"C:\Users\AUNGZAW~1\DOWNLO~1\COMPRES~1\WINDOW~1\Tools\PrcUview\pv.exe" -e 1 1>>"C:\Users\AUNGZAW~1\DOWNLO~1\COMPRES~1\WINDOW~1\AUNGZAWMYO-PC_20211102_133749\LiveResponseData\BasicInfo\PrcUview_extended_long.txt" 2>>"C:\Users\AUNGZAW~1\DOWNLO~1\COMPRES~1\WINDOW~1\AUNGZAWMYO-PC_20211102_133749\AUNGZAWMYO-PC_20211102_133749_Processing_Details.txt"

C:\Users\AungZawMyo\Downloads\Compressed\Windows_Live_Response>"C:\Users\AUNGZAW~1\DOWNLO~1\COMPRES~1\WINDOW~1\Tools\PrcUview\pv.exe" -e 1 1>>"C:\Users\AUNGZAW~1\DOWNLO~1\COMPRES~1\WINDOW~1\AUNGZAWMYO-PC_20211102_133749\LiveResponseData\BasicInfo\PrcUview_extended.txt" 2>>"C:\Users\AUNGZAW~1\DOWNLO~1\COMPRES~1\WINDOW~1\AUNGZAWMYO-PC_20211102_133749\AUNGZAWMYO-PC_20211102_133749_Processing_Details.txt"

***** Module "prcview.bat" has completed. *****
***** Returning to Memory_Dump_Windows_Live_Response.bat *****

*****Running module "Windows-System-Commands.bat" now*****

C:\Users\AungZawMyo\Downloads\Compressed\Windows_Live_Response>chcp 1>>"C:\Users\AUNGZAW~1\DOWNLO~1\COMPRES~1\WINDOW~1\AUNGZAWMYO-PC_20211102_133749\LiveResponseData\BasicInfo\PrcUview_extended.txt" 2>>"C:\Users\AUNGZAW~1\DOWNLO~1\COMPRES~1\WINDOW~1\AUNGZAWMYO-PC_20211102_133749\AUNGZAWMYO-PC_20211102_133749_Processing_Details.txt"
```

ကိုယ်ရွေးချယ်တဲ့ အလုပ်အပေါ်မူတည်ပြီး Result ရဖို့အတွက် အချိန်အတိုင်းအတာ တစ်ခုအထိ ကြာနိုင်ပါတယ်။

I Choice Triage Method.

Windows_Live_Response				
Folder				
Name	Date modified	Type	Size	
AUNGZAWMYO-PC_20211102_133749	11/2/2021 1:37 PM	File folder		
Checklists	3/7/2019 1:54 AM	File folder		
Logos	3/9/2019 2:54 AM	File folder		
Scripts	3/7/2019 3:15 AM	File folder		
Tools	3/7/2019 2:40 AM	File folder		
README-Windows	9/4/2019 11:48 PM	Text Document	13 KB	
Windows Live Response Collection	2/28/2017 12:58 PM	Application	91 KB	
Windows_Complete_Tool_List	3/7/2019 2:40 AM	Microsoft Excel 97...	14 KB	

Result File Location

Windows_Live_Response > AUNGZAWMYO-PC_20211102_133749 > LiveResponseData				
Folder				
Name	Date modified	Type		
BasicInfo	11/2/2021 2:08 PM	File folder		
CopiedFiles	11/2/2021 1:43 PM	File folder		
NetworkInfo	11/2/2021 2:03 PM	File folder		
PersistenceMechanisms	11/2/2021 2:01 PM	File folder		
UserInfo	11/2/2021 1:57 PM	File folder		

Name	Date modified	Type
amcache	11/2/2021 1:43 PM	File
chrome	11/2/2021 1:42 PM	File
eventlogs	11/2/2021 1:40 PM	File
firefox	11/2/2021 1:42 PM	File
hosts	11/2/2021 1:43 PM	File
ie	11/2/2021 1:42 PM	File
logfile	11/2/2021 1:43 PM	File
mft	11/2/2021 1:41 PM	File
prefetch	11/2/2021 1:42 PM	File
recentfilecache	11/2/2021 1:43 PM	File
registry	11/2/2021 1:42 PM	File
SRUMDB	11/2/2021 1:43 PM	File
usnjrnl	11/2/2021 1:40 PM	File
forecopy_handy	11/2/2021 1:43 PM	Text

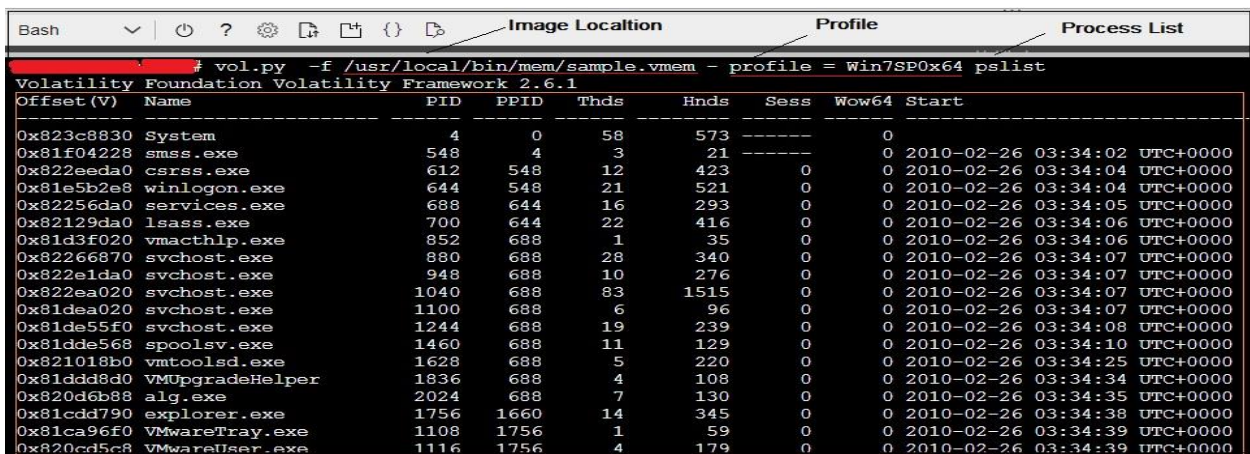
Live Response Data

Memory Forensics Tools

Volatility Frame Work ကတော့ Open Source တစ်ခုဖြစ်ပြီး Commercial Product တွေမှာလဲ Volatility GUI ပုံစံနဲ့ အသုံးပြုပါတယ်။ Memory Image ထည့် Operation System Profile ရွေး။ ကိုယ်စစ်ချင်တဲ့ အကြောင်းအရာကို အဆင်သင့်ရွေးချယ်ရုံပါ။ Kali OS, Parrot OS စတာတွေမှာ Built-In ပါရှိပါတယ်။ RAM Capture လုပ်ဖို့ဆိုရင် FTK Imager, Belkasoft RAM Capture တို့လို့ Tools တွေလဲရှိပါတယ်။ Volatility ကို Window XP-Windows 10, Windows Server 2013-2016, MAC OS 10.5 - 10.15, Linux - OpenSuSE, Ubuntu, Debian, CentOS, Fedora, Mandriva, etc

Volatility ထဲမှာ မပါတဲ့ Operation System Profile အတွက် ကိုယ်တိုင် Profile လုပ်ပြီးထည့်ပေးရမှာ ဖြစ်ပါတယ်။ [Home · volatilityfoundation/volatility Wiki · GitHub](http://Home.volatilityfoundation.org/volatility Wiki)

Support ပေးတဲ့ Memory တွေကတော့ Memory Dump, Windows Crash Dump, Hibernation, Virtual Machine Snapshot တို့ဖြစ်ပါတယ်။ Volatility ကိုစတင်အသုံးပြု မယ်ဆိုရင် Memory Dump ရယူတဲ့ Operation System ရဲ့ Profile ကို သတ်မှတ်ပေးရမှာ ဖြစ်ပါတယ်။ မသိခဲ့ရင်လဲ Volatility မှာ Suggest ပေးပါတယ်။ Memory Dump ရယူတဲ့ Operation System ရဲ့ Profile ကို ကိုယ်က မသိလျှင် မသေချာခဲ့လျှင် imageinfo နဲ့ ရှာနိုင် ပါတယ်။ Profile Name ကို Volatility ရဲ့ Command တိုင်းမှာ --profile အနေနဲ့ ထည့်ပေး ရမှာဖြစ်ပါတယ်။



Offset (V)	Name	PID	PPID	Thds	Hnds	Sess	Wow64	Start
0x823c8830	System	4	0	58	573	-----	0	
0x81f04228	smss.exe	548	4	3	21	-----	0	2010-02-26 03:34:02 UTC+0000
0x822eada0	csrss.exe	612	548	12	423	0	0	2010-02-26 03:34:04 UTC+0000
0x81e5b2e8	winlogon.exe	644	548	21	521	0	0	2010-02-26 03:34:04 UTC+0000
0x82256da0	services.exe	688	644	16	293	0	0	2010-02-26 03:34:05 UTC+0000
0x82129da0	lsass.exe	700	644	22	416	0	0	2010-02-26 03:34:06 UTC+0000
0x81d3f020	vmacthlp.exe	852	688	1	35	0	0	2010-02-26 03:34:06 UTC+0000
0x82266870	svchost.exe	880	688	28	340	0	0	2010-02-26 03:34:07 UTC+0000
0x822e1da0	svchost.exe	948	688	10	276	0	0	2010-02-26 03:34:07 UTC+0000
0x822ea020	svchost.exe	1040	688	83	1515	0	0	2010-02-26 03:34:07 UTC+0000
0x81dea020	svchost.exe	1100	688	6	96	0	0	2010-02-26 03:34:07 UTC+0000
0x81de55f0	svchost.exe	1244	688	19	239	0	0	2010-02-26 03:34:08 UTC+0000
0x81dde568	spoolsv.exe	1460	688	11	129	0	0	2010-02-26 03:34:10 UTC+0000
0x821018b0	vmtoolsd.exe	1628	688	5	220	0	0	2010-02-26 03:34:25 UTC+0000
0x81ddd8d0	VMUPgradeHelper	1836	688	4	108	0	0	2010-02-26 03:34:34 UTC+0000
0x820d6b88	alg.exe	2024	688	7	130	0	0	2010-02-26 03:34:35 UTC+0000
0x81cdd790	explorer.exe	1756	1660	14	345	0	0	2010-02-26 03:34:38 UTC+0000
0x81ca96f0	VMwareTray.exe	1108	1756	1	59	0	0	2010-02-26 03:34:39 UTC+0000
0x820cd5c8	VMwareUser.exe	1116	1756	4	179	0	0	2010-02-26 03:34:39 UTC+0000

Other Forensics Tools

Bulk Extractor ကတော့ Digital Forensics Tools တစ်ခုဖြစ်ပြီး Disk Image, Memory Image, File, Folder တွေကနေ ၎င်းတို့ရဲ့ File System နဲ့ File System Structures ကို မထိခိုက်စေပဲအချက်အလက် Artifacts တွေရှာနိုင်ပါတယ်။ Zip, Rar, Pdf, Word File, JPEG စတာတွေထဲကနေပါ ရှာနိုင်ပါတယ်။ Example - Email, URL, Domain Name, Phone Number, Etc. Bulk Extractor က Kali OS, Parrot OS, SIFT စတာတွေမှာ Built-In ပါရှိပါတယ်။ Bulk Extractor မှာ Report File ကို အလွယ်တကူကြည့်နိုင်ပြီး Summary Report မှာ လဲ Hash Function ပါဝင်ပါတယ်။

```
Bash
/etc# bulk_extractor /usr/local/bin/mem/sample.vmem -o /usr/local/output
bulk_extractor version: 1.6.0-dev
Hostname: .net
Input file: /usr/local/bin/mem/sample.vmem
Output directory: /usr/local/output
Disk Size: 536870912
Threads: 1
Attempt to open /usr/local/bin/mem/sample.vmem
7:22:04 Offset 67MB (12.50%) Done in 0:03:31 at 07:25:35
7:22:37 Offset 150MB (28.12%) Done in 0:02:41 at 07:25:18
7:23:12 Offset 234MB (43.75%) Done in 0:02:06 at 07:25:18
7:23:53 Offset 318MB (59.38%) Done in 0:01:35 at 07:25:28
7:24:56 Offset 402MB (75.00%) Done in 0:01:07 at 07:26:03
7:25:52 Offset 486MB (90.62%) Done in 0:00:26 at 07:26:18
All data are read; waiting for threads to finish...
Time elapsed waiting for 1 thread to finish:
(timeout in 60 min.)
Time elapsed waiting for 1 thread to finish:
6 sec (timeout in 59 min54 sec.)
Thread 0: Processing 520093696

All Threads Finished!
Producer time spent waiting: 272.079 sec.
Average consumer time spent waiting: 0.376292 sec.
*****
** bulk_extractor is probably CPU bound. **
** Run on a computer with more cores **
** to get better performance. **
*****
MD5 of Disk Image: 20d420729287026a3f55704154bd6163
Phase 2. Shutting down scanners
Phase 3. Creating Histograms
Elapsed time: 290.801 sec.
Total MB processed: 536
```

Bulk Extractor Summary Report (Hash - MD5)

```
Bash Bulk-Output
/usr/local/output# ls
aes_keys.txt          elf.txt              find_histogram.txt   ntfsusrn_carved      sin.txt              url_facebook-id.txt   winpe.txt
alerts.txt            email.txt            gps.txt              ntfsusrn_carved.txt  sqlite_carved.txt    url_histogram.txt     winpe_carved
ccn.txt              email_domain_histogram.txt  httplogs.txt         packets.pcap          telephone.txt         url_microsoft-live.txt winpe_carved
ccn_histogram.txt     email_histogram.txt    ip.txt               pii.txt               telephone_histogram.txt url_searches.txt      winprefetch.txt
ccn_track2.txt        ether.txt             ip_histogram.txt     pii_teamviewer.txt   unrar_carved.txt     url_services.txt      zip.txt
ccn_track2_histogram.txt  ether_histogram.txt  jpeg_carved.txt      rar.txt               url.txt              vcard.txt
domain.txt            exif.txt              json.txt             report.xml            url_facebook-address.txt windirs.txt
domain_histogram.txt   find.txt              kml.txt              rfc822.txt            url_facebook-address.txt winlnk.txt
```

Bulk Extractor Report Files

```
Bash
GNU nano 4.8
# BANNER FILE NOT PROVIDED (-b option)
# BULK_EXTRACTOR-Version: 1.6.0-dev ($Rev: 10844 $)
# Feature-Recorder: ip
# Filename: /usr/local/bin/mem/sample.vmem
# Feature-File-Version: 1.1
31900678      192.168.0.176      struct ip R (src) cksum-ok
31900678      239.255.255.250    struct ip L (dst) cksum-ok
32104350      192.168.0.176      struct ip L (src) cksum-ok
32104350      192.168.0.255      struct ip R (dst) cksum-ok
32283766      192.168.0.176      struct ip L (src) cksum-ok
32283766      192.168.0.255      struct ip R (dst) cksum-ok
32698744      192.168.0.176      struct ip L (src) cksum-ok
32698744      72.21.91.19        struct ip R (dst) cksum-ok
36846526      192.168.0.176      struct ip L (src) cksum-ok
36846526      255.255.255.255    struct ip R (dst) cksum-ok
37044238      192.168.0.1        struct ip L (src) cksum-ok
37044238      192.168.0.176      struct ip R (dst) cksum-ok
37046286      192.168.0.176      struct ip L (src) cksum-ok
37046286      192.168.0.1        struct ip L (src) cksum-ok
37048334      192.168.0.176      struct ip R (dst) cksum-ok
37048334      192.168.0.1        struct ip L (src) cksum-ok
37050382      192.168.0.176      struct ip R (dst) cksum-ok
37050382      192.168.0.1        struct ip L (src) cksum-ok
37052430      192.168.0.176      struct ip R (dst) cksum-ok
37052430      193.104.22.71      struct ip R (src) cksum-ok
```

Bulk Extractor Report File -> IP

```
Bash
GNU nano 4.8
# BANNER FILE NOT PROVIDED (-b option)
# BULK_EXTRACTOR-Version: 1.6.0-dev ($Rev: 10844 $)
# Feature-Recorder: telephone
# Filename: /usr/local/bin/mem/sample.vmem
# Histogram-File-Version: 1.1
n=14      8477180400
n=10      4085551234
n=5        496172484
n=2        +14159618830
n=2        8009364200
n=2        9999999999
n=1        012345678901234
n=1        2522277013
n=1        8733735293
```

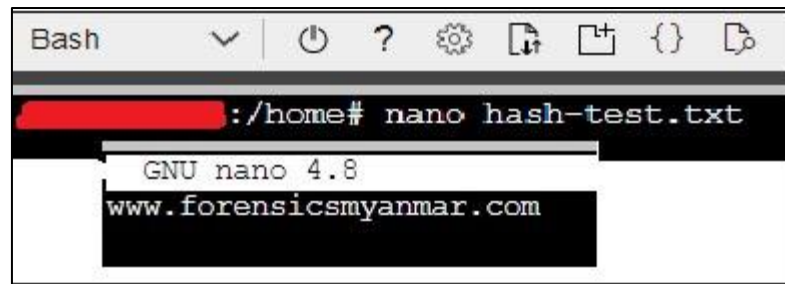
Bulk Extractor Report File -> Telephone (Histogram)

Validating Evidence

Validating Evidence ဆိုတာက Evidence ကို Integrity ရှိအောင်ပြုလုပ်တာဖြစ်ပါတယ်။ Evidence ကို ပြင်ဆင်ဖျက်ဆီးထားရင် Integrity ရှိမှာ မဟုတ်ပါဘူး။ Validating Evidence ကို Hash Function / One Way Cryptographic Functionနဲ့ပြုလုပ်တာဖြစ်ပါတယ်။ တစ်ကယ်လို့ File တစ်ခုခုကို ပြင်ဆင်ဖျက်ဆီးလိုက်ရင် Output Hash တန်ဖိုးက တူညီတော့မှာ မဟုတ်ပါဘူး။ ဒါကြောင့် Hash String ကို Evidence Integrity ရှိ - မရှိ

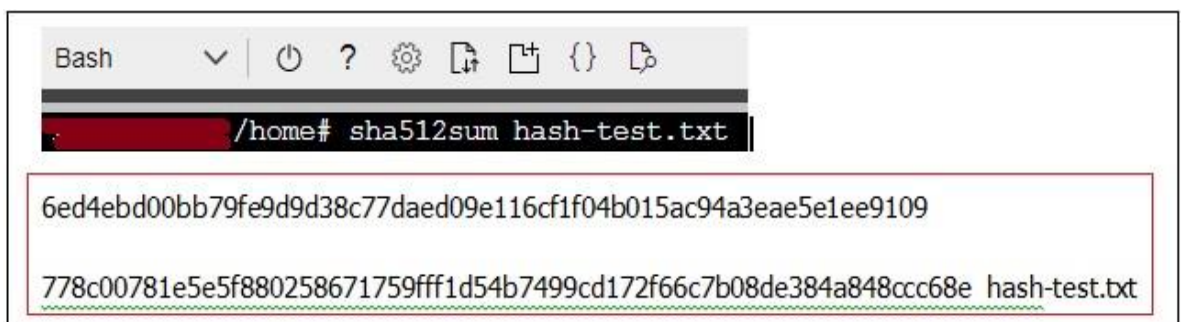
စစ်ဆေးတဲ့နေရာမှာ အသုံးပြု တာဖြစ်ပါတယ်။ ရလာတဲ့ Hash String နဲ့ Storage Media ကို လုံခြုံစွာ သိမ်းဆီးဖို့လဲ အရေးကြီးပါတယ်။ တစ်စုံတစ်ယောက်က ပြင်ဆင်ပြီး Hash String ကို ပြန်ထုတ်သွားနိုင် လို့ဖြစ်ပါတယ်။ Evidence Validating အတွက် Hash Function မျိုးစုံအသုံးပြုပါတယ်။ Hash Function တွေကတော့ ကိုယ်အသုံးပြုတဲ့ Tools , Forensics Imager အပေါ်မှာလဲ မူတည် ပါတယ်။ SHA-1, SHA-2, SHA-3, MD5 . SHA-1 နဲ့ MD5 ကတော့ Secure မဖြစ်တဲ့အတွက် အသုံးမပြုသင့်ပါဘူး။ အချို့နေရာတွေမှာလဲ အသုံးပြုနေဆဲဖြစ်ပါတယ်။

ဥပမာ အနေနဲ့ hash-test.txt ထဲမှာ www.forensicsmyanmar.com လို့ရေး ထားပါတယ်။ အဲဒီ TXT File ကို SHA-512 နဲ့ Hash Value ထုတ်ပါမယ်။ Linux အတွက် sha512sum Command ကိုအသုံးပြုထားပါတယ်။



```
Bash
:/home# nano hash-test.txt
GNU nano 4.8
www.forensicsmyanmar.com
```

hash-test.txt



```
Bash
/home# sha512sum hash-test.txt
6ed4ebd00bb79fe9d9d38c77daed09e116cf1f04b015ac94a3eae5e1ee9109
778c00781e5e5f880258671759fff1d54b7499cd172f66c7b08de384a848ccc68e hash-test.txt
```

1- sha512sum Command & Hash String

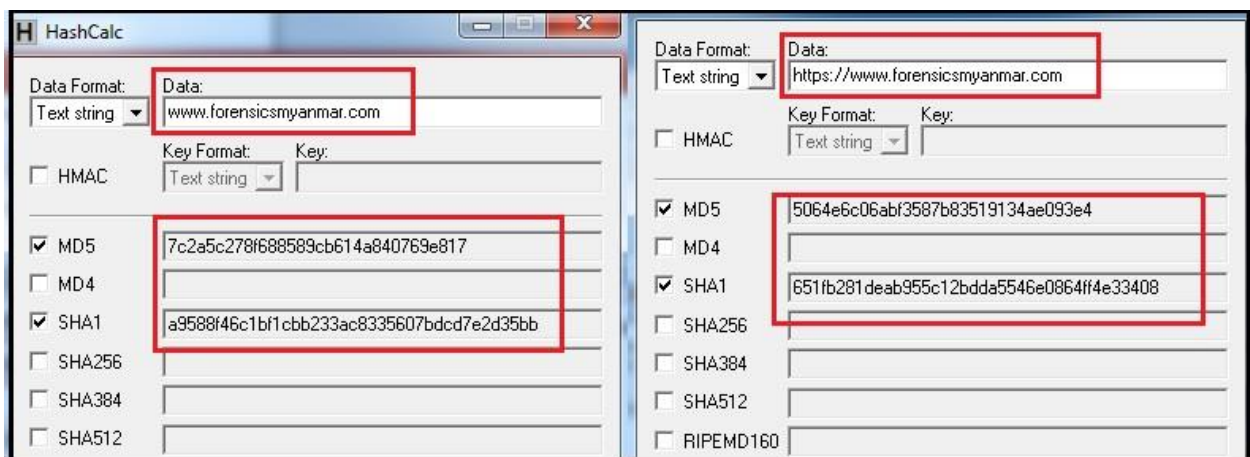
နောက်တစ်ကြိမ် hash-test.txt ထဲမှာ စာတစ်ကြောင်းထပ်တည့်ပြီး SHA-512 နဲ့ Hash Value ပြန်ထုတ်ပါမယ်။ ပထမအကြိမ် Hash String နဲ့ နောက်တစ်ကြိမ် ပြန်ထုတ်တဲ့ Hash String မတူညီတာကို တွေ့ရပါလိမ့်မယ်။

```
Bash
GNU nano 4.8
www.forensicsmyanmar.com
Digital Forensics

Bash
[redacted]:/home# cat hash-test.txt
www.forensicsmyanmar.com
Digital Forensics

[redacted]:/home# sha256sum hash-test.txt
aed67b8e3db0b0d75196f58a5c2097ccadf67c22c34abfe729c73952e7c8f722 hash-test.txt
[redacted]:/home#
```

Course ထဲမှာ Window အတွက် Hash Calc ကိုအသုံးပြုထားပါတယ်။
စာလုံးပြောင်း သွားတာနဲ့ Hash String ပြောင်းလဲသွားတာကို တွေ့နိုင်ပါတယ်။



Hash Calculator

ဒါကြောင့် ကျွန်တော်တို့ Evidence ကို မပျက်စီး မပြင်ဆင်နိုင်အောင် Acquisition လုပ်တိုင်းမှာ Evidence Integrity အတွက် Hash Value ပြုလုပ်ရတာဖြစ်ပါတယ်။ Hash Value ထုတ်ပြီးနောက်ပိုင်း Storage Media ကို သေချာစွာ သိမ်းဆည်းထားရမှာ ဖြစ်ပါတယ်။

Exploring Evidence

Forensics Image နဲ့ Hash Value ရယူပြီးနောက်တစ်ဆင့်ကတော့ Evidence Analysis ဒါမှမဟုတ် Explore လုပ်ဖို့ဖြစ်ပါတယ်။ Storage ထဲမှာ ဘာတွေရှိမလဲ

ဘယ်လိုလုပ် ရမယ်ဆိုတာကို နည်းလမ်းရယူဖို့ ဖြစ်ပါတယ်။ အဲဒီလိုပြုလုပ်ဖို့အတွက် Evidence ကို Workstation နဲ့ချိတ်ဆက်ရမှာ ဖြစ်ပါတယ်။

အရင်သင်ခန်းစာတွေအရ Evidence က Forensics Image သို့မဟုတ် Clone Drive ဖြစ်နိုင်ပါတယ်။ ဒါကြောင့် Evidence ချိတ်ဆက်ဖို့အတွက် Workstation မှာ မတူညီတဲ့ နည်းလမ်းတွေကို အသုံးပြုရမှာ ဖြစ်ပါတယ်။ Evidence တွေက File System မျိုးစုံရှိနိုင် တဲ့အတွက် Workstation က File System နဲ့ တူဖို့လိုအပ်ပါတယ်။

ချိတ်ဆက်ဖို့က သာမန်လုပ်နေကျအတိုင်း Mount ပြုလုပ်တာဖြစ်ပါတယ်။ USB Or Docking နဲ့ Workstation ကို ချိတ်ဆက်ခြင်းဖြစ်ပါတယ်။ ဒါပေမဲ့ Evidence Storage Or Forensics Image ကို Read-Only အနေနဲ့သာ Mount လုပ်တာဖြစ်ပါတယ်။ Evidence Storage Or Forensics Image ထဲမှာ အမှားအယွင်းတစ်စုံတစ်ခုလုပ်မိခြင်းမှ ကာကွယ်နိုင်ဖို့ ဖြစ်ပါတယ်။ ဒါကြောင့် Read + Write Mode အနေနဲ့ မပြုလုပ် မိဖို့အရေးကြီးပါတယ်။

Evidence Storage Or Forensics Image ကို Mount လုပ်ပြီးတဲ့အချိန်မှာ Storage Or Forensics Image ထဲက အချက်အလက်တွေကို မြင်နိုင် ကြည့်နိုင်မှာဖြစ်ပါတယ်။ ဘာလို့လဲ ဆိုရင် Read-Only အနေနဲ့ပြုလုပ်ထားလို့ ဖြစ်ပါတယ်။ Read-Only Mount ကို Linux မှာလဲပြုလုပ်နိုင်သလို Workstation က Window ဖြစ်နေရင် FTK Imager, Mount Image Pro, OSFmount, Arsenal Image Mounter တို့ကို အသုံးပြုနိုင်ပါတယ်။

Kali, Paladin, Parrot စတဲ့ Operation System တွေကို Forensics Mode အနေနဲ့ အသုံးပြုရင် လာချိတ်ဆက်သမျှ Storage Media မှန်သမျှက Read-Only Mode အနေနဲ့သာ အလုပ်လုပ်ပါတယ်။

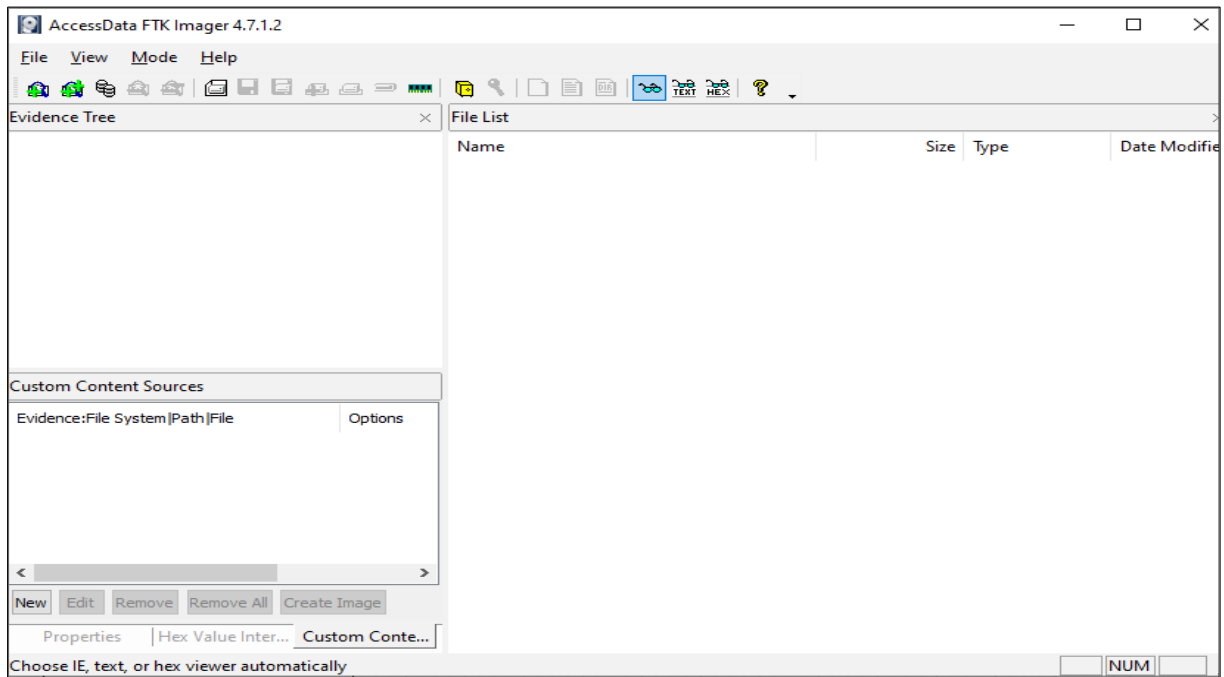
အခုလောက်ဆိုရင် Acquisition Process အကြောင်းကို နားလည်သဘောပေါက်မယ် လို့ယူဆပါတယ်။ နည်းစနစ်တွေကတော့ နိုင်ငံအလိုက် ဥပဒေ နည်းဥပဒေ အလိုက် ကွဲပြားမှု ရှိပေမဲ့ တော်တော်များများ ကတော့ ပုံစံတူညီပါတယ်။

အခု PDF မှာတော့ FTK Imager အသုံးပြုနည်းကို ဖော်ပြသွားမှာဖြစ်ပါတယ်။ FTK Imager က Access Data ကနေပြုလုပ်ထားတဲ့ Open Source Forensics Imager တစ်ခုဖြစ်ပါတယ်။ FTK Imager ကိုအသုံးပြုပြီး လုပ်ဆောင်နိုင်တာတွေကို အောက်မှာဖော်ပြထားပေးပါတယ်။

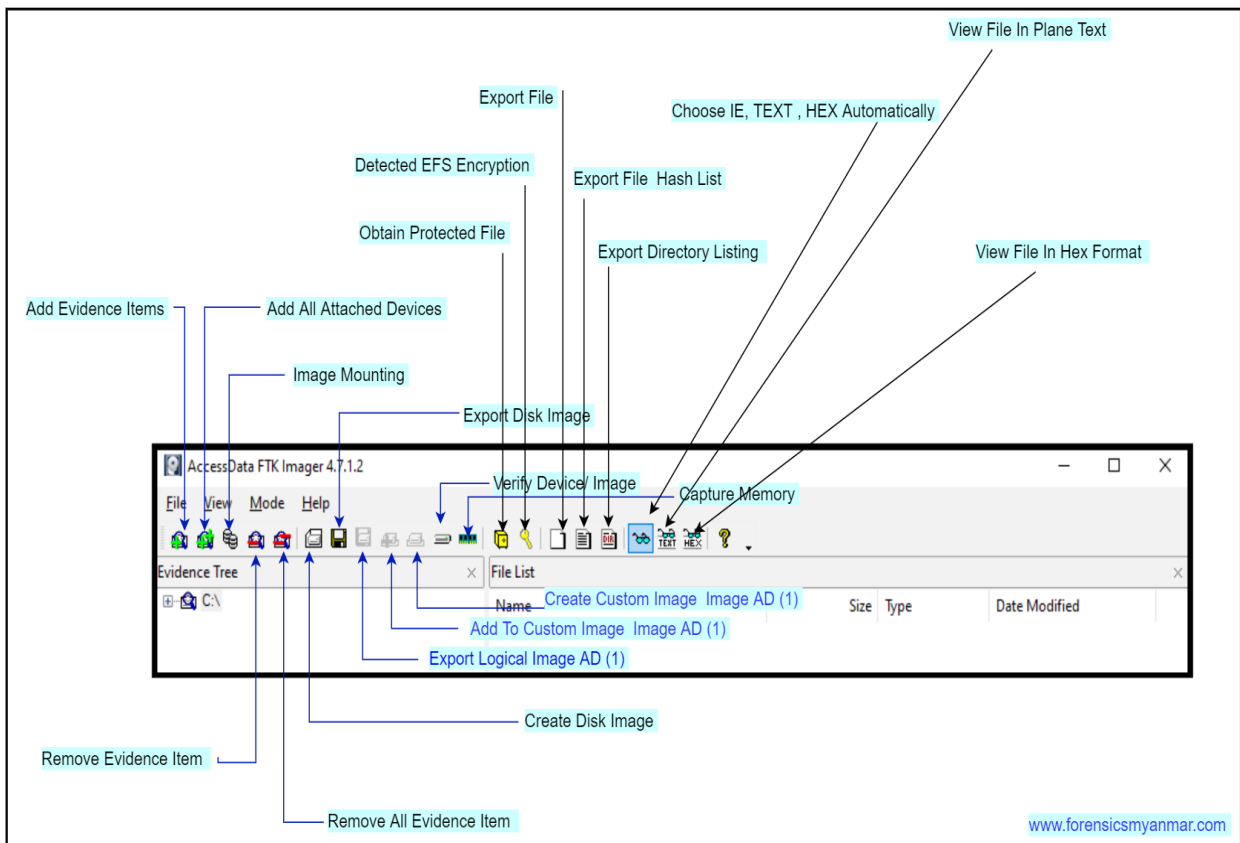
- Forensics Image ပြုလုပ်ခြင်း။
- Forensics Image ကို Mount ပြုလုပ်ခြင်း။
- Forensics Image ထဲကနေ File Or Folder တွေကို Export ပြုလုပ်ခြင်း။
- Disk Or Storage Devices တွေထဲကနေ ကိုယ် Analysis လုပ်ချင်တဲ့ အပိုင်းကိုပဲ Image ပြုလုပ်ခြင်း။
- System Live ဖြစ်နေတဲ့အချိန် Protected ဖြစ်နေတဲ့ System File တွေကို ရယူခြင်း။
- Image File & Storage တွေကို Analysis ပြုလုပ်နိုင်ခြင်း။
- System Live Memory Dump ရယူနိုင်ခြင်း။
- Protected Registry Files များရယူနိုင်ခြင်း။
- Image Integrity အတွက် Hash ပြုလုပ်နိုင်ခြင်း။
- EFS Encryption ကို Detect ပြုလုပ်နိုင်ခြင်း။
- အခြားသော Feature များ။

Software Imager ကိုအသုံးပြုတတ်မယ်ဆိုရင် Hardware Imager တွေကိုပါ လွယ်ကူစွာ အသုံးပြုနိုင်ပါတယ်။ FTK Imager ကိုတော့ အောက်ဖော်ပြပါ လင့်ကနေ Free Download ပြုလုပ်နိုင်ပါတယ်။ MB 50 ပဲရှိပါတယ်။

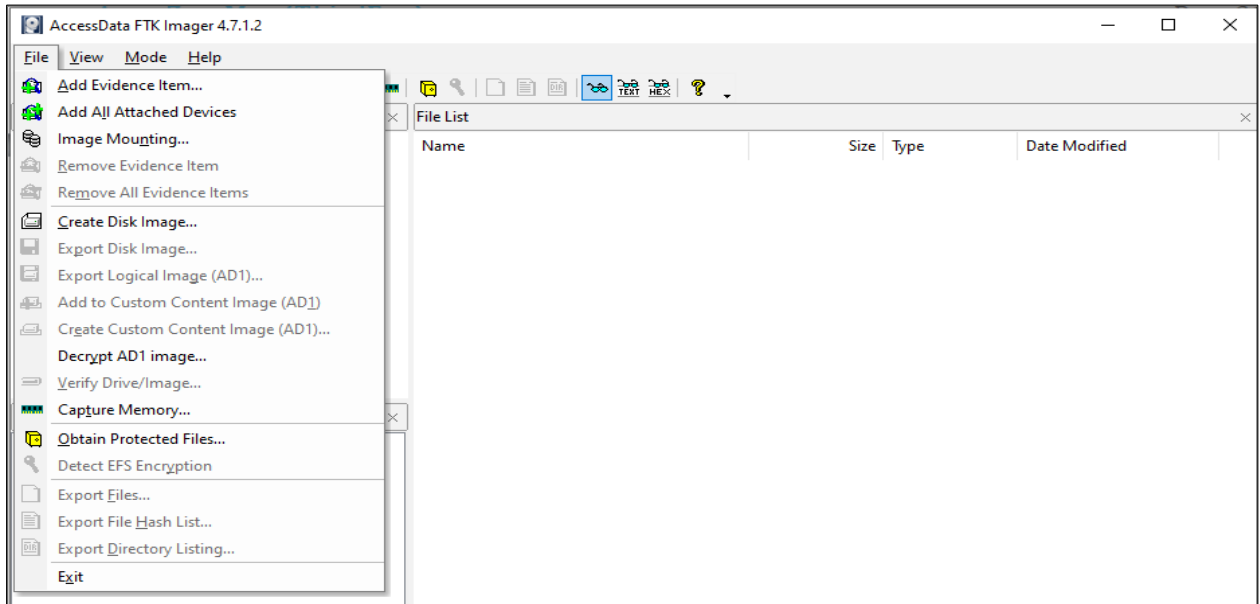
Download FTK Imager = <https://go.exterro.com/l/43312/2022-01-21/f6h1s3>



FTK Imager Main View



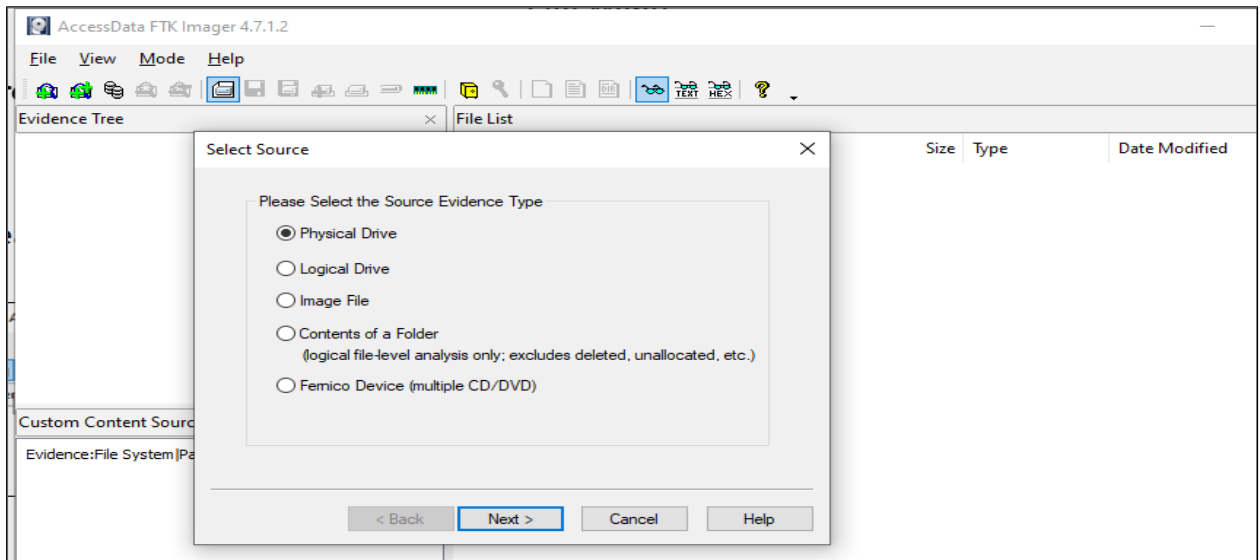
FTK Imager Tool Bar



File Menu

Forensics Image ပြုလုပ်ခြင်း

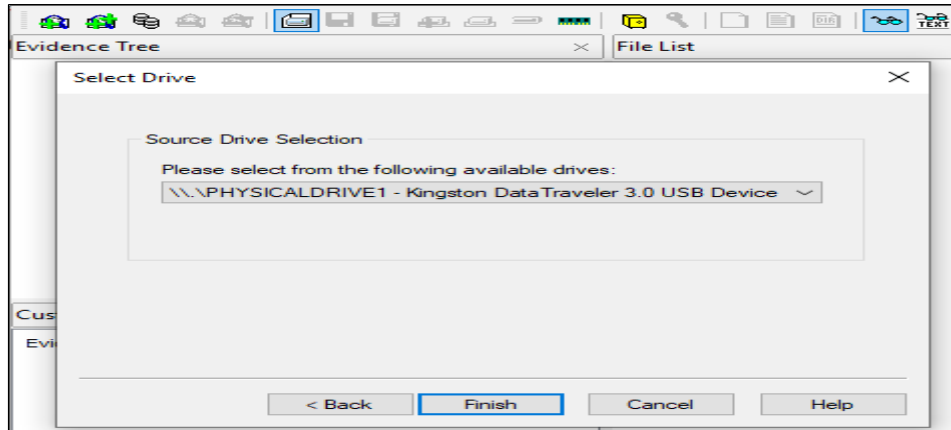
Forensics Image ပြုလုပ်ဖို့အတွက် Tool bar မှ Create Disk Image ကနေလဲပြုလုပ် လို့ရသလို File Menu ကနေလဲပြုလုပ်လို့ရပါတယ်။



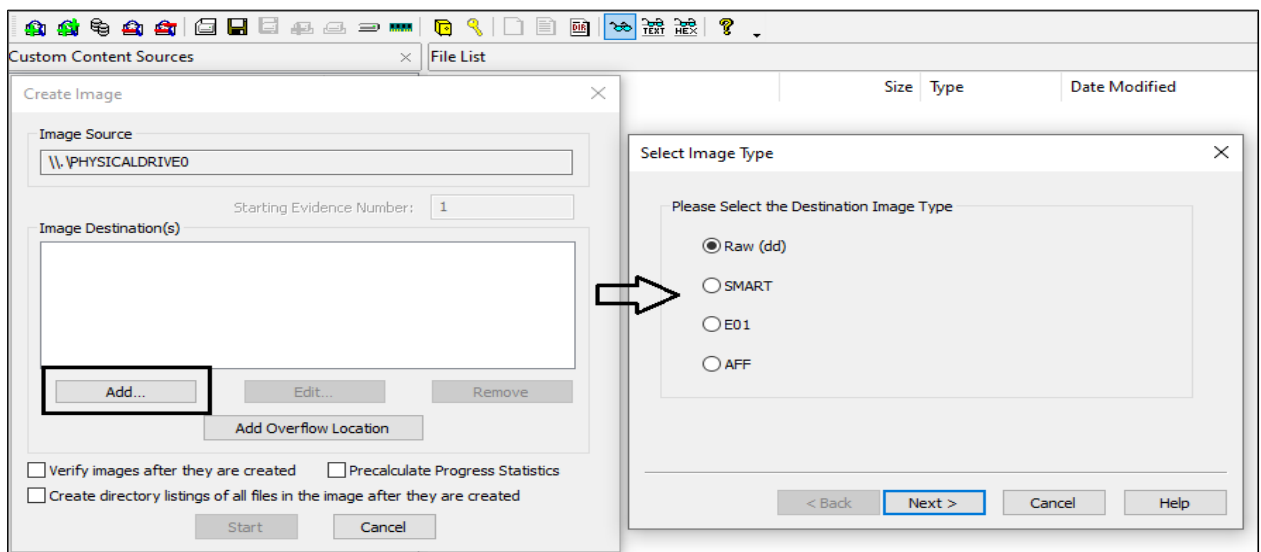
Tool Bar > Create Disk Image

အဲဒီအချိန်မှာ Select Source ဆိုပြီး Box တစ်ခုပေါ်လာပါမယ်။ ဒါကတော့ Image ရယူမဲ့ Source Device ကို ရွေးခိုင်းတာဖြစ်ပါတယ်။ Physical Device ကတော့ ကိုယ် Image

ရယူမဲ့ Device တစ်ခုလုံးကို ဆိုလိုတာဖြစ်ပါတယ်။ ပုံမှန်ဆိုရင် ကွန်ပျူတာနဲ့ Storage တစ်ခုလုံးရယ် USB Stick တစ်ခုရယ်ကိုတွေ့ရမှာဖြစ်ပါတယ်။ လက်တွေ့မှာဆိုရင်တော့ ကိုယ် Image ရယူမည့် Device ကိုရွေးရမှာဖြစ်ပါတယ်။ ဥပမာအနေနဲ့ USB Stick ကို Forensics Image ယူပြပါမယ်။



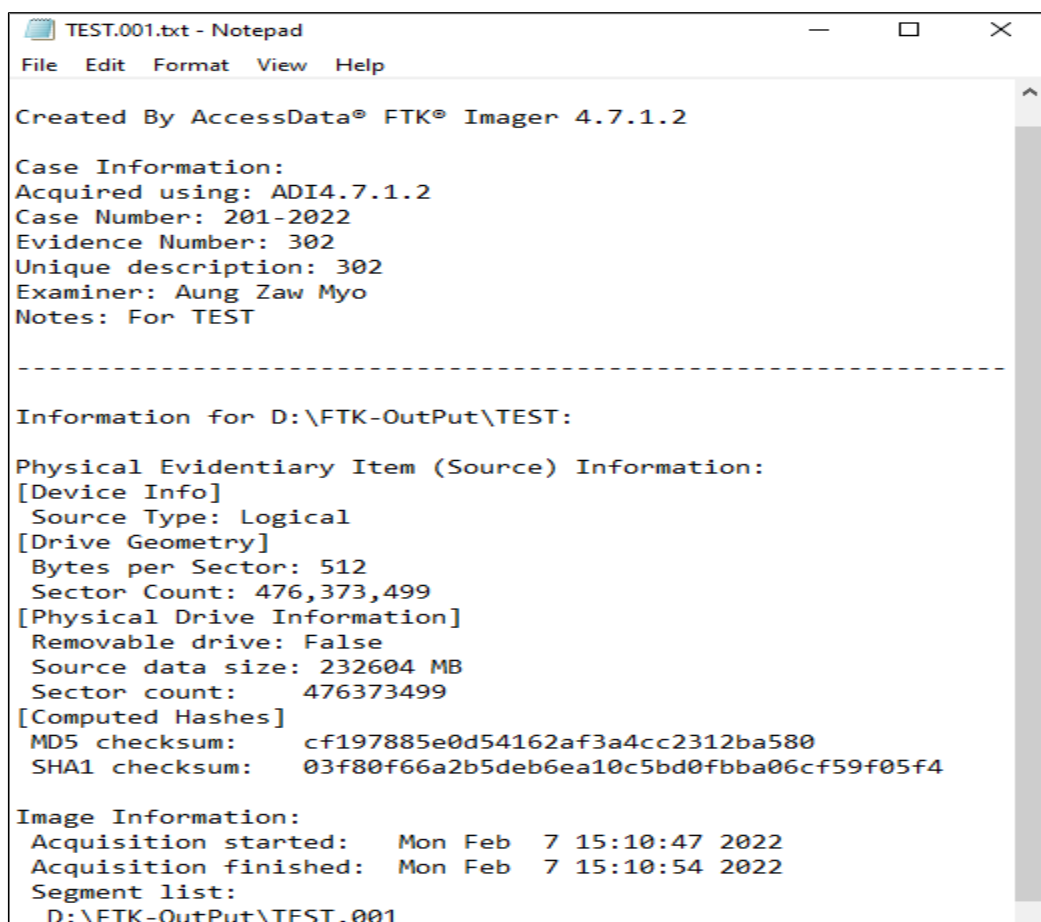
Selecte Your Source Device



အပေါ်ကပုံမှာဆိုရင် Image Destination (add) ကိုနှိပ်လိုက်ရင် ဘယ်လိုမျိုး Forensics Image Format ကို ရယူမယ်ဆိုတာကို ရွေးချယ်ဖို့အတွက် Box တစ်ခုပေါ်လာပါလိမ့်မယ်။ အခုအခါမှာတော့ Raw (dd) ကို Image Format အဖြစ်ရွေးထားပါတယ်။

Raw (DD) ကတော့ Storage တစ်ခုလုံး ဒါမှမဟုတ် Logical Volume တစ်ခုလုံးကို Bit By Bit (Raw) အနေနဲ့ ကူးယူတာဖြစ်ပါတယ်။ RAW (DD) နဲ့ Forensics Image ပြုလုပ်ရင် Image File ရဲ့ Metadata အချက်အလက်က အချို့ Toolsတွေမှာပါဝင်တာရှိ

သလို မပါဝင်တာလဲရှိပါတယ်။ FTK မှာတော့ Image File ရဲ့ Metadata တွေပါဝင်ပါတယ်။ RAW Format ကိုတော့ မည်သည့် Forensics Software မဆို Support လုပ်ပါတယ်။ Image File ရဲ့ Metadata ဆိုတာကို အောက်ကပုံမှာ နမူနာပြထားပါတယ်။ Image File ရဲ့ Metadata ထဲမှာ Case Information, Acquire လုပ်တဲ့ Application Name, Output Location, Storage Information, Acquire လုပ်တဲ့ Storage Size, Hash Value, ဘယ်နေ့ဘယ်အချိန်မှာ Forensics Image ပြုလုပ်တယ် ဘယ်အချိန်မှာ Image လုပ်တဲ့ Process ပြီးဆုံးတယ် စတဲ့ အချက်အလက်တွေ ပါဝင်ပါတယ်။ Linux မှာလဲ DD Command သုံးပြီး ပြုလုပ်နိုင်ပါတယ်။



```
TEST.001.txt - Notepad
File Edit Format View Help

Created By AccessData® FTK® Imager 4.7.1.2

Case Information:
Acquired using: ADI4.7.1.2
Case Number: 201-2022
Evidence Number: 302
Unique description: 302
Examiner: Aung Zaw Myo
Notes: For TEST

-----

Information for D:\FTK-OutPut\TEST:

Physical Evidentiary Item (Source) Information:
[Device Info]
Source Type: Logical
[Drive Geometry]
Bytes per Sector: 512
Sector Count: 476,373,499
[Physical Drive Information]
Removable drive: False
Source data size: 232604 MB
Sector count: 476373499
[Computed Hashes]
MD5 checksum: cf197885e0d54162af3a4cc2312ba580
SHA1 checksum: 03f80f66a2b5deb6ea10c5bd0fbba06cf59f05f4

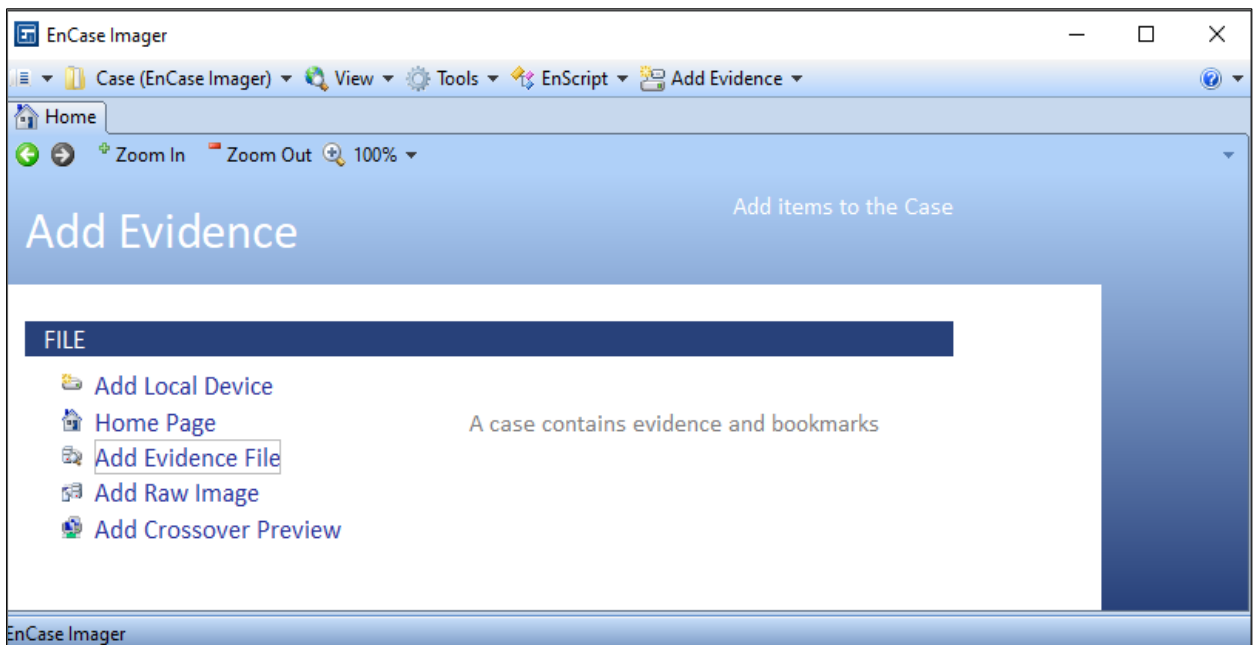
Image Information:
Acquisition started: Mon Feb 7 15:10:47 2022
Acquisition finished: Mon Feb 7 15:10:54 2022
Segment list:
D:\FTK-OutPut\TEST.001
```

Forensics Image File Metadata Information

SMART ဆိုတာက SMARTLinux မှာအသုံးပြုတဲ့ Forensics Image Format ဖြစ်ပါတယ်။ SMARTLinux ကိုတော့ အခုအချိန်မှာ US မှာရှိတဲ့ Law Enforcement , ထောက်လှမ်း ရေး၊ တပ်နဲ့ဆက်စပ်တဲ့လုပ်ငန်းတွေမှာပဲ အသုံးပြုလို့ရပါတော့တယ်။ FTK Imager မှာတော့ SMART Format ကိုဖွင့်ပြီး Analysis ပြုလုပ်လို့ရပါတယ်။ နောက်ပိုင်းမှာ

Image File ကိုဖွင့်ပြီး Analysis ပြုလုပ်တာ ကိုယ်လိုချင်တဲ့ File Or Folder ကိုပဲ Custom Image ရယူတာ၊ Export လုပ်တာတွေ ဖော်ပြသွားပါမယ်။

E01 ကတော့ Encase Forensics ရဲ့ Forensics Image တစ်ခုဖြစ်ပါတယ်။ Encase Forensics ကိုအသုံးပြုပြီးပဲ Analysis ပြုလုပ်လို့ရအောင်ပြုလုပ်ထားတာဖြစ်ပါတယ်။ နောက်ပိုင်းမှာတော့ E01 Format ကို အခြား Forensics Commercial Product တွေမှာလဲ Support ပေးလာပြီးဖြစ်ပါတယ်။ Encase မှာလဲ သူ့အတွက် သီးသန့် Imager ရှိပါတယ်။ FTK Imager ကနေ E01 Format ရနိုင်သလို။ E01 Forensics Image Format ကိုလဲ Imager မှာဖွင့် လို့ရပါတယ်။ တစ်ခုကိုကောင်းကောင်းသုံးတတ်ရင်ကျန်တဲ့ ဘယ်လိုမျိုးပဲ လာလာ အဆင် ပြေပါတယ်။

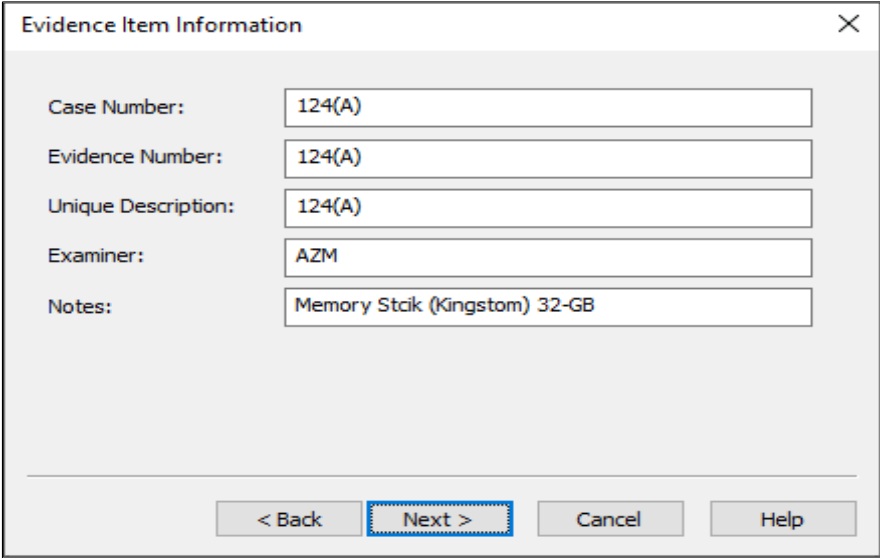


Encase Imager

Advanced Forensics Format (AFF) ကတော့ Open Source တစ်ခုဖြစ်ပါတယ်။ အခုအခါမှာတော့ AFF4 ထွက်ရှိနေပြီးဖြစ်ပါတယ်။ Block လိုက်ကူးယူခြင်း၊ လိုအပ်တဲ့ အပိုင်းကိုသာကူးယူနိုင်ခြင်း၊ Sparse Data တွေမပါခြင်းကြောင့် ပိုပြီးမြန်ဆန်ပါတယ်။ Mac Forensisc ပြုလုပ်တဲ့နေရာမှာ SSD SATA, M2, Memory Stick တွေကို Acquire လုပ်တဲ့ နေရာမှာ အဓိကသုံးစွဲပါတယ်။ Mac Forensisc Tools ဖြစ်တဲ့ Blackbag မှာ AFF4 ကို သုံးစွဲပါတယ်။ Sleuthkit မှာလဲ Support ပေးပါတယ်။ AFF4 ကို 7 Zip နဲ့လဲဖွင့်နိုင်ပါတယ်။ AFF အကြောင်း ပိုပြီးကြည့်နိုင်ဖို့အတွက်

<https://www.forensicsmyanmar.com/2020/12/ssd-acquisition.html>

နောက်တစ်ဆင့်ကိုသွားမယ်ဆိုရင် ကိုယ်စစ်ဆေးမဲ့ Case Information ကိုဖြည့်ရမဲ့ အပိုင်းဖြစ်ပါတယ်။ ဒီအချက်အလက်တွေက Forensics Image ရဲ့ Metadata မှာ ပါဝင်မှာ ဖြစ်ပါတယ်။

A screenshot of the 'Evidence Item Information' dialog box. It contains five text input fields: 'Case Number' with '124(A)', 'Evidence Number' with '124(A)', 'Unique Description' with '124(A)', 'Examiner' with 'AZM', and 'Notes' with 'Memory Stick (Kingston) 32-GB'. At the bottom, there are four buttons: '< Back', 'Next >', 'Cancel', and 'Help'. The 'Next >' button is highlighted with a blue dashed border.

Case Information

နောက်တစ်ဆင့်ကတော့ Image ကိုထားမဲ့ Destination နဲ့ Image File Name ကိုဖြည့် စွက်ရမှာဖြစ်ပါတယ်။ E01, Smart, AFF Format ကိုရွေးမယ်ဆိုရင် Compression လုပ်တဲ့နှုန်းကို သတ်မှတ်ပေးလို့ရပါတယ်။ အခုက DD Format ကိုသာရွေးထားပါတယ်။

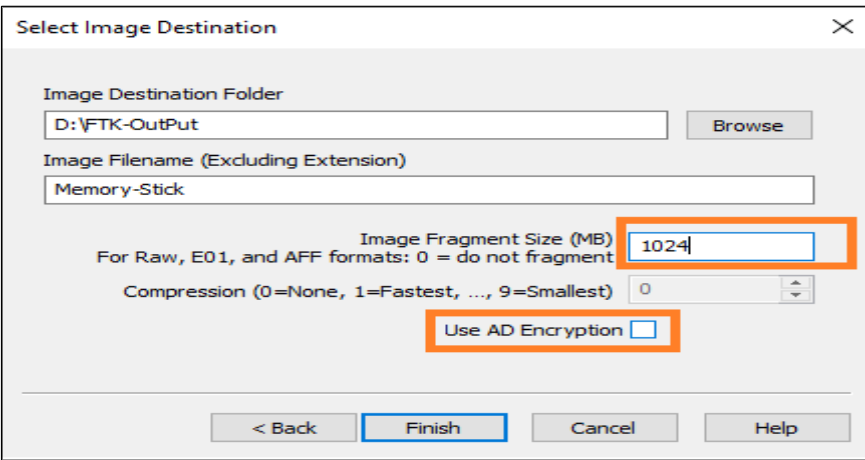
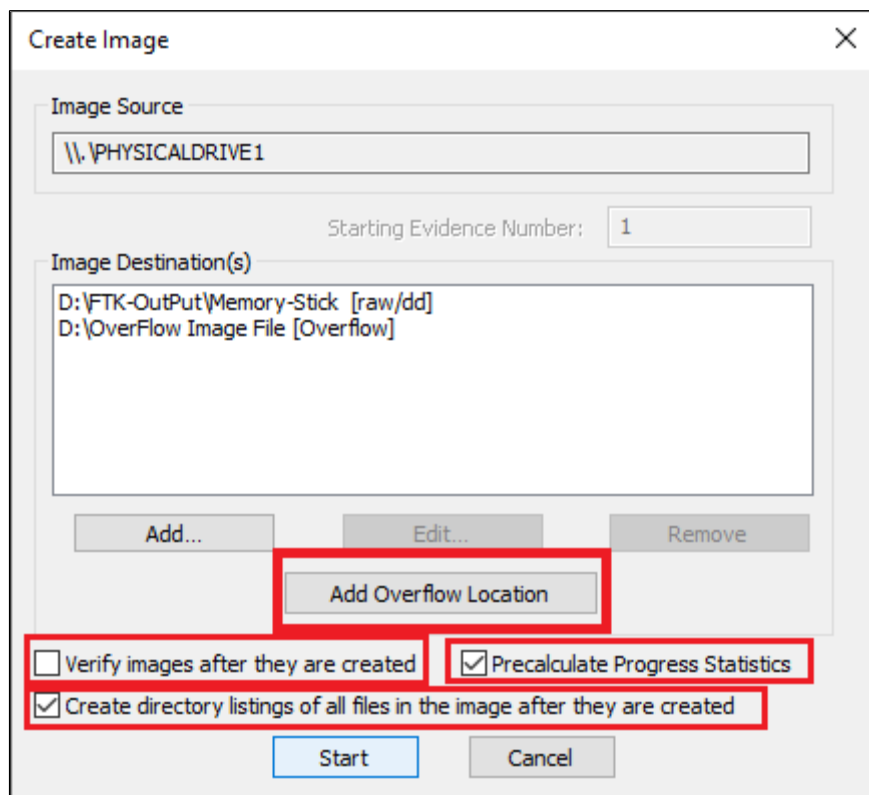
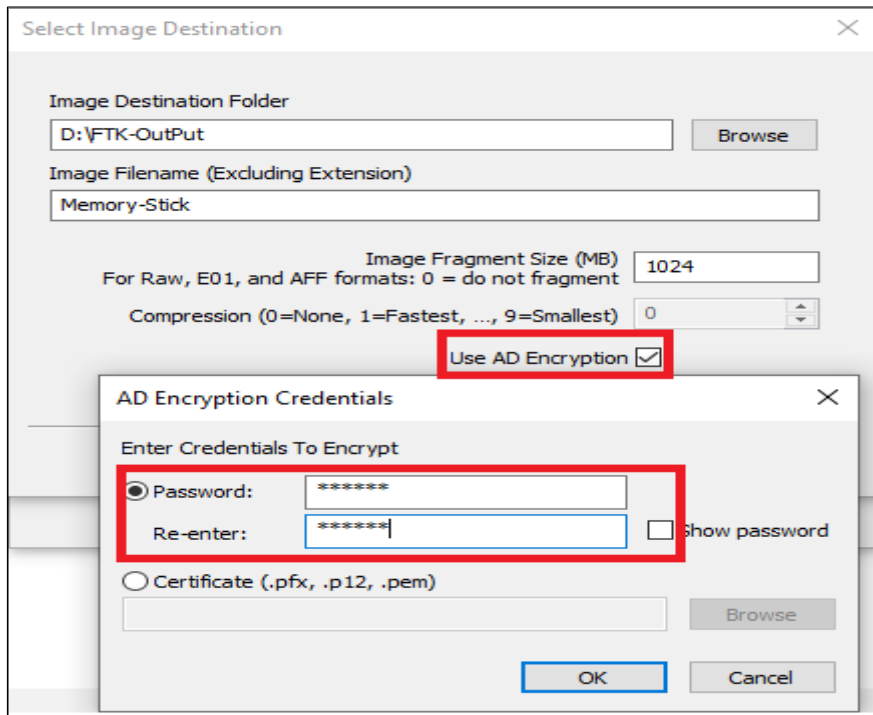
A screenshot of the 'Select Image Destination' dialog box. It has two text input fields: 'Image Destination Folder' with 'D:\FTK-OutPut' and 'Image Filename (Excluding Extension)' with 'Memory-Stick'. Below these are three settings: 'Image Fragment Size (MB)' set to '1024', 'Compression (0=None, 1=Fastest, ..., 9=Smallest)' set to '0', and 'Use AD Encryption' with an unchecked checkbox. The '1024' and 'Use AD Encryption' fields are highlighted with orange boxes. At the bottom, there are four buttons: '< Back', 'Finish', 'Cancel', and 'Help'. The 'Finish' button is highlighted with a blue dashed border.

Image Fragment လုပ်တယ်ဆိုတာကတော့ Image File ကို အစိတ်အပိုင်း လေးတွေ ခွဲလိုက်တာဖြစ်ပါတယ်။ ဒီနေရာမှာဆိုရင် 32 GB ကို 1024 MB အနေနဲ့ နမူနာခွဲပြထား

ပေးပါတယ်။ Use AD Encryption ဆိုတာကတော့ Forensics Image File ကို လူတိုင်း Access လုပ်လို့မရနိုင်စေရန်အတွက် Password ပေးတာဖြစ်ပါတယ်။



Add Overflow Location ဆိုတာကတော့ Forensics Image ကို တစ်နေရာထဲမဟုတ်ပဲ ကျန်တဲ့ နေရာမှာပါခွဲပြီး Image လုပ်တာဖြစ်ပါတယ်။ တစ်ခါတည်း Image File (2) ခုရရှိအောင်ပြုလုပ်တာဖြစ်ပါတယ်။ Verify Image After They are Created ဆိုတာက မူရင်း Storage Media ကိုရော Forensics Image ကိုရော Hash Value တိုက်စစ် တာဖြစ်ပါတယ်။ Create Directory Listing Of All Files in The Image After They are Crated ဆိုတာကတော့ Storage Media ထဲမှာရှိတဲ့ File, Folder တွေကို List အနေနဲ့ Export ထုတ်မယ် လို့ဆို လိုတာဖြစ်ပါတယ်။ Precalculate Progress Statistics ဆိုတာက Image လုပ်တဲ့အခါမှာ ကြာမြင့်နိုင်တဲ့ အချိန်ကိုဖော်ပြခိုင်းတာဖြစ်ပါတယ်။ Add Overflow Location ကိုရွေးမယ်ဆိုရင် တော့ Verify Image မလုပ်နိုင်ပါဘူး။ Imager က နေရာတစ်ခုထဲကိုပဲ Image Verify လုပ်ပေး နိုင်ပါတယ်။ **အခုအခါမှာတော့ Image File တစ်ခုသာပြုလုပ်ထားပါတယ်။**

အောက်ကပုံမှာဆိုရင် 1 Second ကို 87 MB လောက်နှုန်းနဲ့ 32 GB ကို 5 မိနစ်ကျော် လောက်ကြာမှာဖြစ်ပါတယ်။ Hardware Imager တွေကိုသုံးမယ်ဆိုရင်တော့ အခုအချိန်ထက် ပိုပြီး မြန်ဆန်မှာ ဖြစ်ပါတယ်။ Image Summary ကိုကြည့်လိုက်မယ်ဆိုရင် Forensics Image ရဲ့ Metadata အချက်အလက်တွေကိုတွေ့နိုင်မှာဖြစ်ပါတယ်။ Forensics Image Metadata တွေက Output နေရာမှာလဲ Text File အနေနဲ့ရှိပါတယ်။ Output Folder မှာမြင်ရမဲ့ Forensics Image ပုံစံကိုပြသထားပါတယ်။ File တစ်ခုကို အပေါ်မှာ 1 GB စီခွဲထားခဲ့ပါတယ်။ **Create Directory Listing Of All Files In The Image After They are Crated** ကိုရွေးထားခဲ့အတွက် Image File ထဲက File, Folder တွေအကြောင်းကို CSV File အနေနဲ့ထုတ်ပေးမှာဖြစ်ပါတယ်။ CSV File ထဲမှာ Image File ထဲမှာရှိတဲ့ File တစ်ခုချင်းစီရဲ့ File Name, File Path, File Size, File ကို Create လုပ်တဲ့အချိန်၊ File ကို Accessed လုပ်တဲ့အချိန်၊ အခုလုပ်တဲ့ Storage Media ထဲမှာ File ကို ဖျက်ထားလား မဖျက်ထားဘူးလား ဆိုတဲ့ အချက်အလက်တွေ ပါဝင်ပါတယ်။ Text File ထဲမှာဆိုရင် Storage Media ရဲ့ အချက်အလက်၊ Compute Hash ဖြစ်တဲ့ Stroage Media ရဲ့ မူရင်း Hash၊ Forensics Image စတင်ပြုလုပ်တဲ့အချိန်နှင့် ပြီးစီးတဲ့အချိန်၊ Image Verification Result ဖြစ်တဲ့ Forensics Image File ရဲ့ Hash တွေကိုတွေ့ရမှာဖြစ်ပါတယ်။ **မူရင်း Storage Media ရဲ့ Hash နဲ့ Image File ရဲ့ Hash တို့တူညီနေရမှာဖြစ်ပါတယ်။**

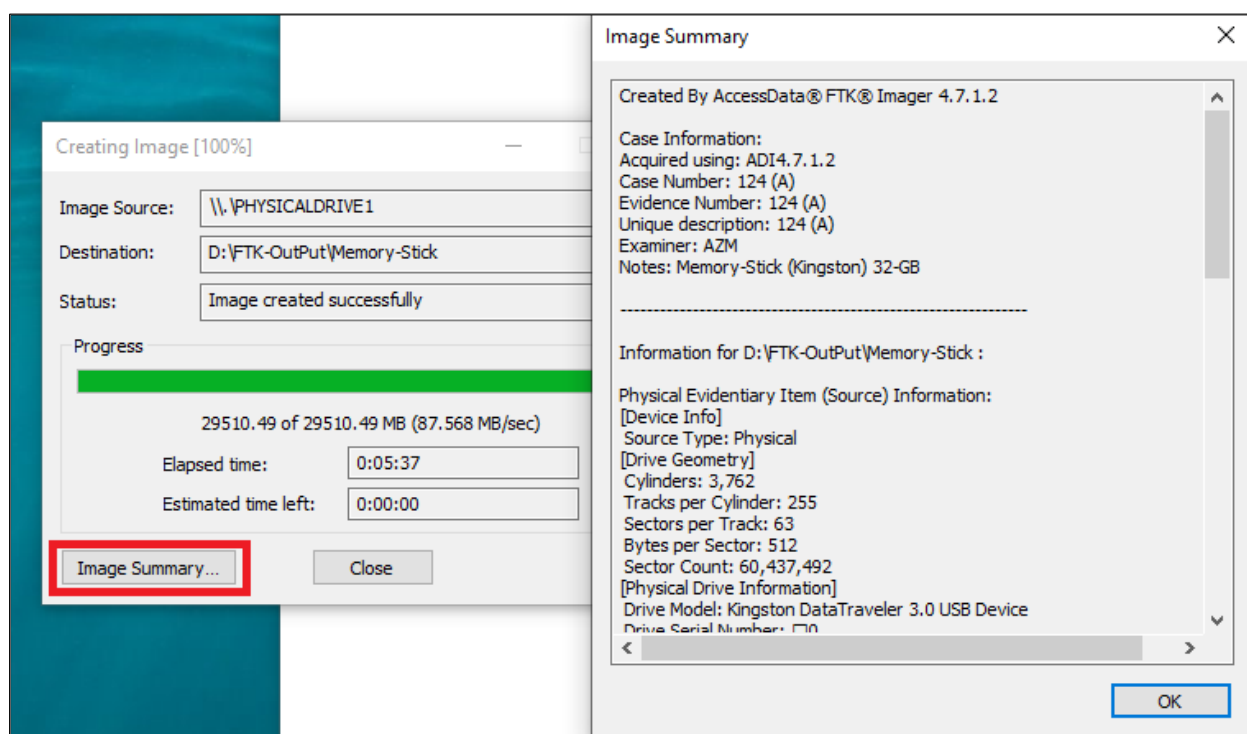


Image Summary

Name	Date modified	Type	Size
Memory-Stick .001	2/8/2022 10:23 AM	WinRAR archive	1,048,577 KB
Memory-Stick .001.csv	2/8/2022 10:29 AM	Microsoft Excel C...	6,001 KB
Memory-Stick .001.txt	2/8/2022 10:33 AM	Text Document	3 KB
Memory-Stick .002	2/8/2022 10:23 AM	002 File	1,048,576 KB
Memory-Stick .003	2/8/2022 10:23 AM	003 File	1,048,576 KB
Memory-Stick .004	2/8/2022 10:24 AM	004 File	1,048,576 KB
Memory-Stick .005	2/8/2022 10:24 AM	005 File	1,048,576 KB
Memory-Stick .006	2/8/2022 10:24 AM	006 File	1,048,576 KB
Memory-Stick .007	2/8/2022 10:24 AM	007 File	1,048,576 KB
Memory-Stick .008	2/8/2022 10:24 AM	008 File	1,048,576 KB
Memory-Stick .009	2/8/2022 10:25 AM	009 File	1,048,576 KB
Memory-Stick .010	2/8/2022 10:25 AM	010 File	1,048,576 KB
Memory-Stick .011	2/8/2022 10:25 AM	011 File	1,048,576 KB
Memory-Stick .012	2/8/2022 10:25 AM	012 File	1,048,576 KB
Memory-Stick .013	2/8/2022 10:25 AM	013 File	1,048,576 KB
Memory-Stick .014	2/8/2022 10:26 AM	014 File	1,048,576 KB
Memory-Stick .015	2/8/2022 10:26 AM	015 File	1,048,576 KB
Memory-Stick .016	2/8/2022 10:26 AM	016 File	1,048,576 KB
Memory-Stick .017	2/8/2022 10:26 AM	017 File	1,048,576 KB
Memory-Stick .018	2/8/2022 10:26 AM	018 File	1,048,576 KB
Memory-Stick .019	2/8/2022 10:27 AM	019 File	1,048,576 KB
Memory-Stick .020	2/8/2022 10:27 AM	020 File	1,048,576 KB
Memory-Stick .021	2/8/2022 10:27 AM	021 File	1,048,576 KB
Memory-Stick .022	2/8/2022 10:27 AM	022 File	1,048,576 KB
Memory-Stick .023	2/8/2022 10:27 AM	023 File	1,048,576 KB
Memory-Stick .024	2/8/2022 10:28 AM	024 File	1,048,576 KB
Memory-Stick .025	2/8/2022 10:28 AM	025 File	1,048,576 KB
Memory-Stick .026	2/8/2022 10:28 AM	026 File	1,048,576 KB
Memory-Stick .027	2/8/2022 10:28 AM	027 File	1,048,576 KB
Memory-Stick .028	2/8/2022 10:28 AM	028 File	1,048,576 KB
Memory-Stick .029	2/8/2022 10:29 AM	029 File	858,618 KB

Forensics Image Output

	Filename	Full Path	Size (bytes)	Created	Modified	Accessed	Is Deleted
1							
2	[root]	Partition 1\NONAME [FAT32]\[root]\	16384				no
3	VBR	Partition 1\NONAME [FAT32]\VBR	512				no
4	reserved sectors	Partition 1\NONAME [FAT32]\reserved sectors	1675776				no
5	[unallocated space]	Partition 1\NONAME [FAT32]\[unallocated space]\	0				no
6	FAT1	Partition 1\NONAME [FAT32]\FAT1	7550464				no
7	FAT2	Partition 1\NONAME [FAT32]\FAT2	7550464				no
8	FTK Imager	Partition 1\NONAME [FAT32]\[root]\FTK Imager\	16384	2022-Feb-04 15:24:43.460000	2022-Jan-21 14:25:04		no
9	EZ-Tools (1+2) Aung Zaw Myo.pdf	Partition 1\NONAME [FAT32]\[root]\EZ-Tools (1+2) Aung Zaw Myo.pdf	2999199	2022-Feb-04 17:41:45.040000	2022-Feb-04 17:32:04		no
10	Imager	Partition 1\NONAME [FAT32]\[root]\Imager\	16384	2021-Nov-11 11:36:14.930000	2022-Feb-06 17:32:18		yes
11	1643883084950 (1).pdf	Partition 1\NONAME [FAT32]\[root]\1643883084950 (1).pdf	2878550	1980-Jan-01 00:05:15.120000	1980-Jan-01 00:05:04		no
12	297477_Ghosts of Ozarks 2022 1080p 6CH (CM).n	Partition 1\NONAME [FAT32]\[root]\1644297477_Ghosts of Ozarks 2022 1080p 6CH (C	1348443706	2022-Feb-07 16:32:16.800000	2022-Feb-07 16:30:44		yes
13	4113664_The.Ledge.2022.1080p.WEB-DL[CM].non	Partition 1\NONAME [FAT32]\[root]\1644113664_The.Ledge.2022.1080p.WEB-DL[CM	1121976320	2022-Feb-07 16:35:22.850000	2022-Feb-07 16:35:24		yes
14	06667_Special.Delivery.2022.1080p.WEB-DL.CM	Partition 1\NONAME [FAT32]\[root]\1644206667_Special.Delivery.2022.1080p.WEB-DL	1634813233	2022-Feb-07 16:39:13.170000	2022-Feb-07 16:37:18		yes
15	New Kung Fu Cult Master II 2022 WEB-DL 1080p	Partition 1\NONAME [FAT32]\[root]\1644146292_New Kung Fu Cult Master II 2022 WEB-DL	2008114595	2022-Feb-07 16:42:02.420000	2022-Feb-07 16:38:46		yes

Output CSV (File , Folder Information)

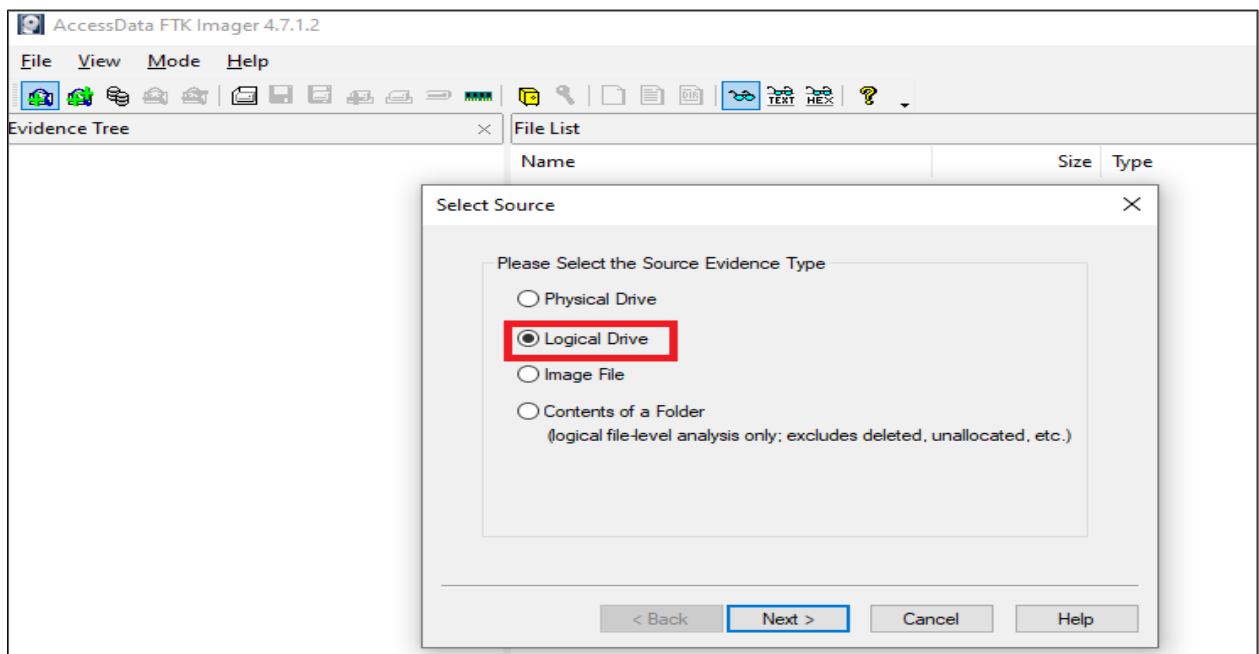
Memory-Stick .001.txt - Notepad File Edit Format View Help Cylinders: 3,762 Tracks per Cylinder: 255 Sectors per Track: 63 Bytes per Sector: 512 Sector Count: 60,437,492 Physical Drive Information] Drive Model: Kingston DataTraveler 3.0 USB Device Drive Serial Number: [0 Drive Interface Type: USB Removable drive: True Source data size: 29510 MB Sector count: 60437492 Computed Hashes] MD5 checksum: c2adbe46d6fffb8c4a938b4a2118b14c SHA1 checksum: 7951beba99d0e785b6965fc81b0e1e847c194b82 Image Information: Acquisition started: Tue Feb 8 10:23:23 2022 Acquisition finished: Tue Feb 8 10:29:00 2022 Segment list. D:\FTK-Output\Memory-Stick .001 D:\FTK-Output\Memory-Stick .002 D:\FTK-Output\Memory-Stick .003 D:\FTK-Output\Memory-Stick .004 D:\FTK-Output\Memory-Stick .005 D:\FTK-Output\Memory-Stick .006 D:\FTK-Output\Memory-Stick .007 D:\FTK-Output\Memory-Stick .008 D:\FTK-Output\Memory-Stick .009 D:\FTK-Output\Memory-Stick .010 D:\FTK-Output\Memory-Stick .011		D:\FTK-Output\Memory-Stick .012 D:\FTK-Output\Memory-Stick .013 D:\FTK-Output\Memory-Stick .014 D:\FTK-Output\Memory-Stick .015 D:\FTK-Output\Memory-Stick .016 D:\FTK-Output\Memory-Stick .017 D:\FTK-Output\Memory-Stick .018 D:\FTK-Output\Memory-Stick .019 D:\FTK-Output\Memory-Stick .020 D:\FTK-Output\Memory-Stick .021 D:\FTK-Output\Memory-Stick .022 D:\FTK-Output\Memory-Stick .023 D:\FTK-Output\Memory-Stick .024 D:\FTK-Output\Memory-Stick .025 D:\FTK-Output\Memory-Stick .026 D:\FTK-Output\Memory-Stick .027 D:\FTK-Output\Memory-Stick .028 D:\FTK-Output\Memory-Stick .029 Image Verification Results: Verification started: Tue Feb 8 10:29:03 2022 Verification finished: Tue Feb 8 10:33:33 2022 MD5 checksum: c2adbe46d6fffb8c4a938b4a2118b14c : verified SHA1 checksum: 7951beba99d0e785b6965fc81b0e1e847c194b82 : verified	
---	--	---	--

Image File Information (Forensics Image Metadata Text File)

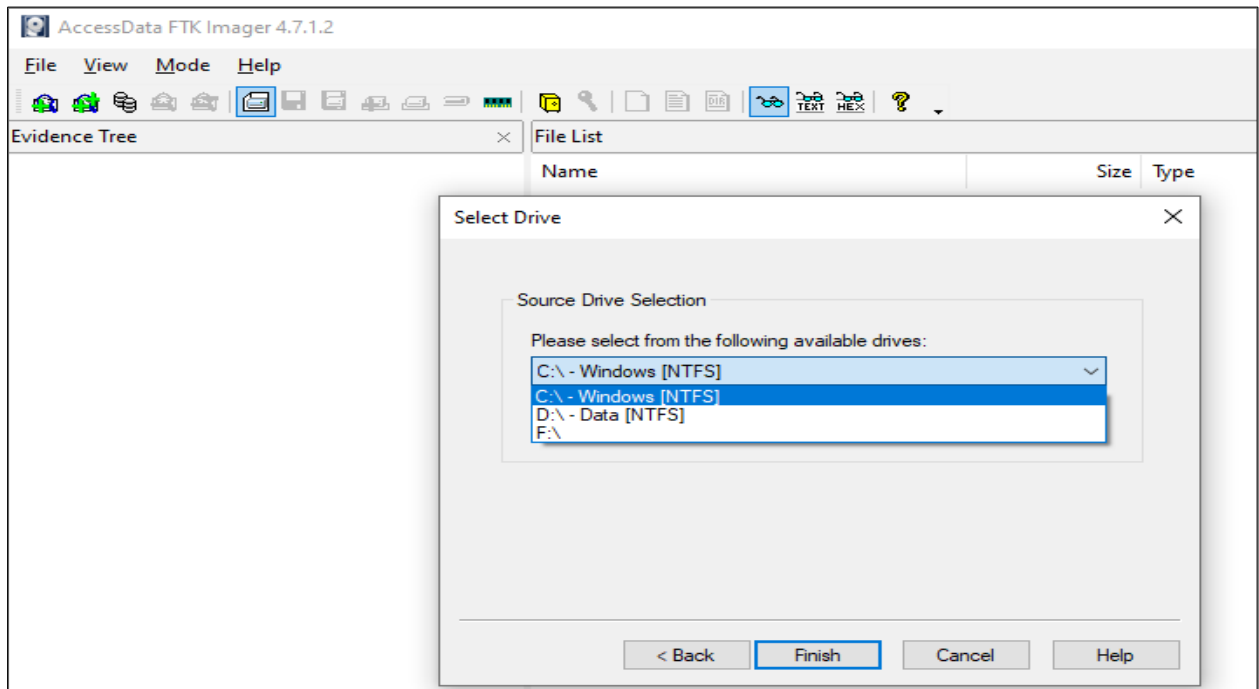
Forensics Image ပြုလုပ်ခြင်း (Logical)

Logical Image ပြုလုပ်ရတဲ့အကြောင်းအရင်းကတော့ Storage တစ်ခုမှာ Partition အနေနဲ့ ၂ ခု ဒါမှမဟုတ် ၃ ခုအထိရှိနိုင်ပါတယ်။ လိုအပ်ချက်အရသော်လည်းကောင်း၊ အချိန်မရှိ တဲ့အခါမှာသော်လည်းကောင်း၊ ကိုယ်ယူမဲ့ Evidence တွေက ဒီနေရာမှာ ရှိတယ်လို့ ယူဆရင် သော်လည်းကောင်း၊ သေချာတဲ့အခါမှာသော်လည်းကောင်း၊ အဲဒီလိုအခြေအနေ မျိုးတွေမှာ Logical Image ကိုပြုလုပ်တာဖြစ်ပါတယ်။

ပြုလုပ်နည်းကတော့ အပေါ်မှာရေးထားတာတွေနဲ့ပုံစံအတူတူပဲ ဖြစ်ပါတယ်။ Image လုပ်မဲ့ Device ကနေ Logical Drive ကိုရွေးချယ်ပြီးပြုလုပ်ရမှာဖြစ်ပါတယ်။ ပုံမှာတော့ C:\ Logical Image အနေနဲ့ရယူတာကိုပြသထားပါတယ်။



Logical Drive



Choice Partition C:\ OR D:\ OR F:\

Forensics Image ကို Mount ပြုလုပ်ခြင်း

Forensics Image ကို Mount ပြုလုပ်တယ်ဆိုတာကတော့ Image File ကို ပုံမှန် မြင်နေကျ Drive တစ်ခုအနေနဲ့ မြင်သာအောင် Read Only အနေနဲ့ကြည့်နိုင်အောင် ပြုလုပ်တာဖြစ်ပါတယ်။ Tool bar ကနေသော်လည်း ကောင်း File Menu ကနေသော်လည်းကောင်း ပြုလုပ်နိုင် ပါသည်။ Mount ပြုလုပ်နိုင်တဲ့ Forensics Image Format တွေကတော့ RAW/dd images, E01, S01, AFF, AD1, L01 စတဲ့ Format တွေဖြစ်ပါတယ်။

AD1, S01 Image File Format တွေကတော့ Custom Image တွေဖြစ်တဲ့အတွက် Full File Structure ပါဝင်ပြီး Geometry Or other physical drive data တွေမပါဝင်တဲ့အတွက် Physical Mount ပြုလုပ်လို့မရနိုင်ပါ။ Logical Mount သာပြုလုပ် လို့ရပါမယ်။

E01, S01, AFF, 001 (RAW/dd) image File တွေကတော့ Drive Image တွေဖြစ်ပြီး Disk, Partitions, File Structure , Drive Data တွေပါဝင်ပါတယ်။ Physical Mount ပြုလုပ်လို့ရပါမယ်။ Mount ပြုလုပ်ပြီး ပုံမှန် Window ကနေလွယ်လွယ်ကူကူကြည့်နိုင်ခြင်း၊

ကြည့်တဲ့အခါမှာ Ready Only Mode ကြောင့် Evidence မပျက်စီးနိုင်ခြင်း၊ Mount ပြုလုပ်ထားတဲ့ Drive ကနေ File တွေကိုကူးယူပြီး အခြား Analysis အတွက် အသုံးပြုနိုင်ခြင်း၊ Mount Image ပေါ်မှာ anti-virus Run နိုင်ခြင်းစတာတွေ ပြုလုပ်နိုင်ပါတယ်။

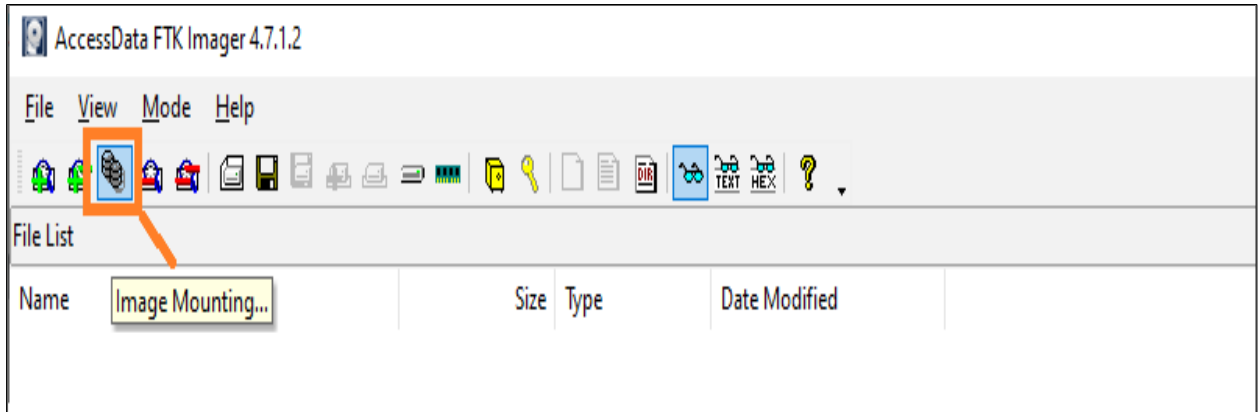
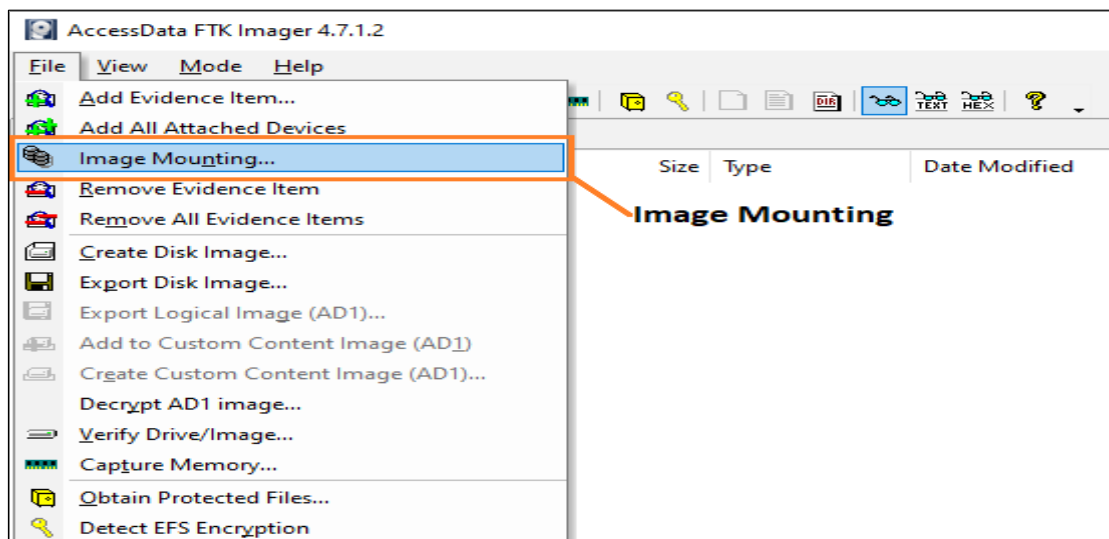
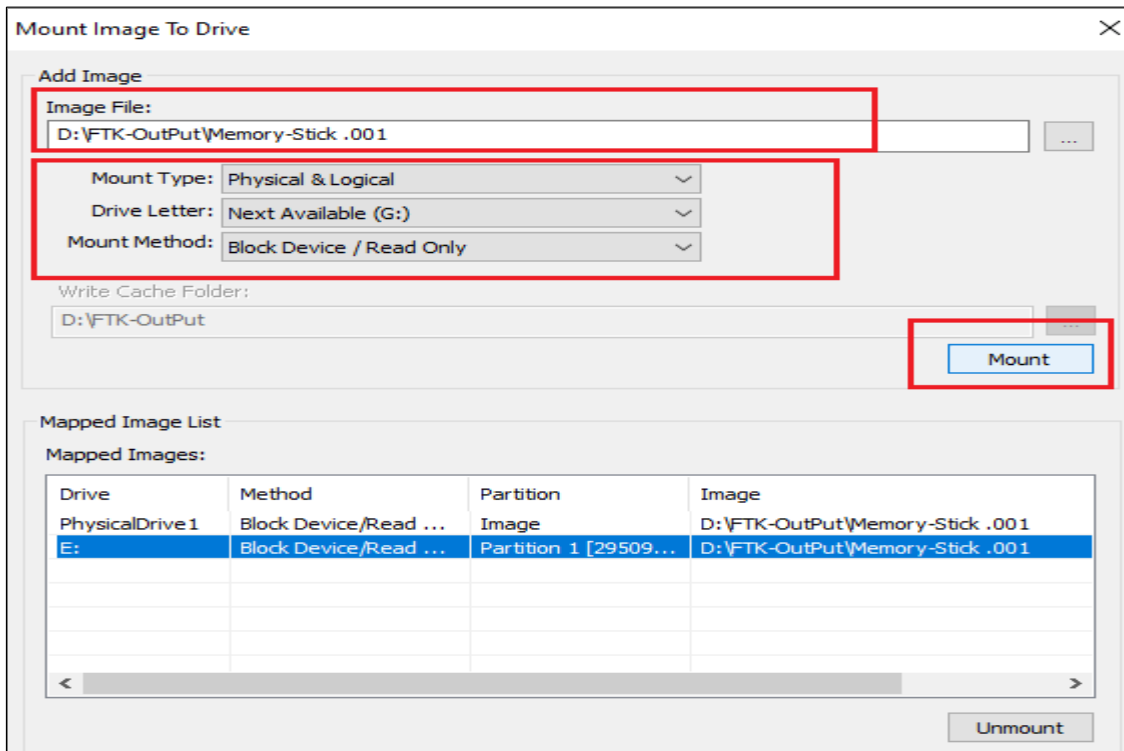


Image Mounting

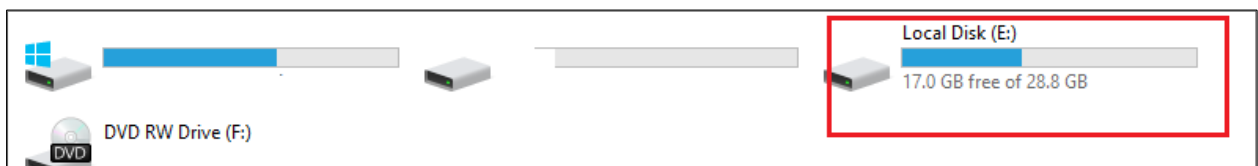


File Menu > Image Mounting

Image Mounting လုပ်မယ်ဆိုရင် Image File ရှိတဲ့ location နေရာကိုရွေးချယ်ပါမယ်။ Image File က Password Protect လုပ်ထားရင် Password ထည့်ပေးပါမယ်။ အခုအချိန်မှာ တော့ Mount Type ကို Physical & Logical နဲ့ဘယ်လို Image ပဲလာလာ Mount လို့ရအောင် ရွေးထားပါတယ်။



Drive Letter ကိုတော့ ကိုယ်အဆင်ပြေသလိုရွေးချယ်လို့ရပါတယ်။ Mount Method ကိုတော့ Read Only Mode အနေနဲ့သာ Mount ပြုလုပ်ထားပါတယ်။ Read Only Mode ဖြစ်တဲ့အတွက် Mount ပြုလုပ်ထားတဲ့ Drive ကို Analysis ပြုလုပ်ရင် ဒါမှမဟုတ် ကြည့်နေရင်းနဲ့ အမှားအယွင်းတစ်စုံတစ်ရာ မဖြစ်အောင်၊ အထဲက File တွေဖျက်လို့ ပြင်လို့ မရအောင်၊ အထဲကို File တွေထပ်ပြီထည့်တာ ပြုလုပ်လို့ မရစေရန် အတွက် ဖြစ်ပါတယ်။ Mount ပြုလုပ်လိုက်ရင် အောက်ကပုံအတိုင်း မြင်ရမှာ ဖြစ်ပါတယ်။ အလုပ်ပြီးပြီးဆိုရင်တော့ FTK Imager ကနေ Unmount ပြုလုပ်ပေးရမှာ ဖြစ်ပါတယ်။ File System အနေနဲ့လဲ Mount ပြုလုပ်ပြထားပါတယ်။ File System (Read only) အနေနဲ့ Mount ပြုလုပ်ရင် Data တွေက Root Folder ထဲမှာရှိမှာဖြစ်ပါတယ်။



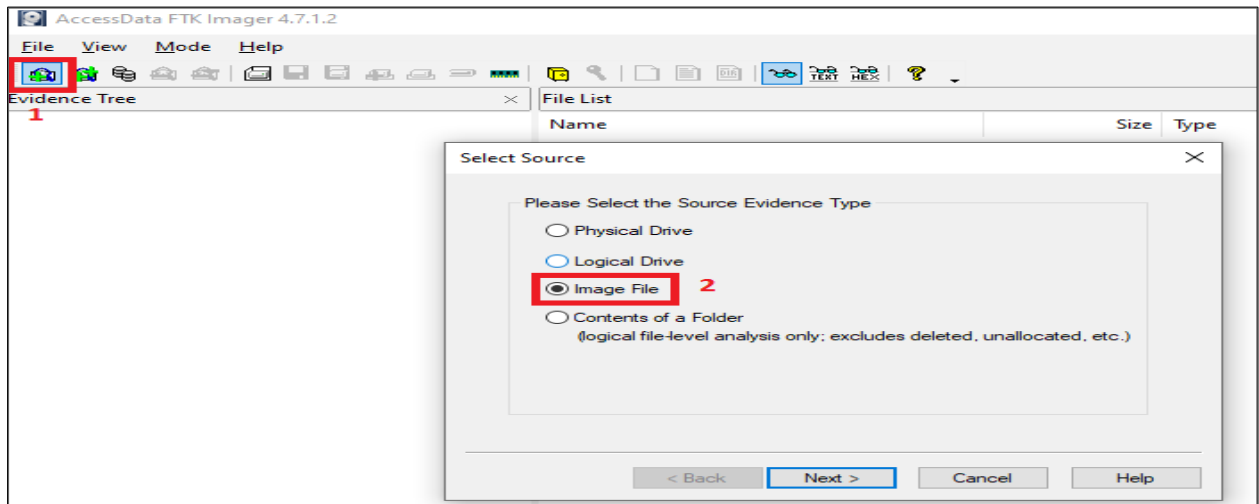
This PC > Local Disk (E:) >				
Name	Date modified	Type	Size	
AZ-304T00A-Trainer-Files-Microsoft-Azur...	1/17/2022 10:01 AM	File folder		
FTK Imager	1/21/2022 2:25 PM	File folder		
Kaspersky	1/11/2022 8:16 AM	File folder		
New folder	2/3/2022 4:26 PM	File folder		
1643883084950 (1).pdf		Adobe Acrobat D...	2,812 KB	
EZ-Tools (1+2) Aung Zaw Myo.pdf	2/4/2022 5:32 PM	Adobe Acrobat D...	2,929 KB	
		Adobe Acrobat D...	363 KB	

This PC > Removable Disk (E:) >				
Name	Date modified	Type	Size	
[root]		File folder		
[unallocated space]		File folder		
FAT1		File	7,374 KB	
FAT2		File	7,374 KB	
reserved sectors		File	1,637 KB	
VBR		File	1 KB	

File System (Read Only Mount)

Forensics Image ထဲကနေ File Or Folder တွေကို Export ပြုလုပ်ခြင်း

Forensics Image ထဲကနေ File Or Folder တွေကို Export ပြုလုပ်ဖို့အတွက် အရင်ဆုံး Forensics Image ကို Add လုပ်ပါမယ်။ Forensics Image File မဟုတ်ပဲ အခြား Physical Device, Logical Device, Folder တွေထဲကနေလဲ Export ပြုလုပ်လို့ရပါတယ်။ Tool bar ကနေ Add Evidence Items ကိုနှိပ်ပြီး Image File အမျိုးအစားကိုရွေးချယ်ပါ။ ပြီးရင် Image File ရှိတဲ့ Location ကနေ Image File ကိုရယူပါမယ်။



Add Evidence Items, Image File

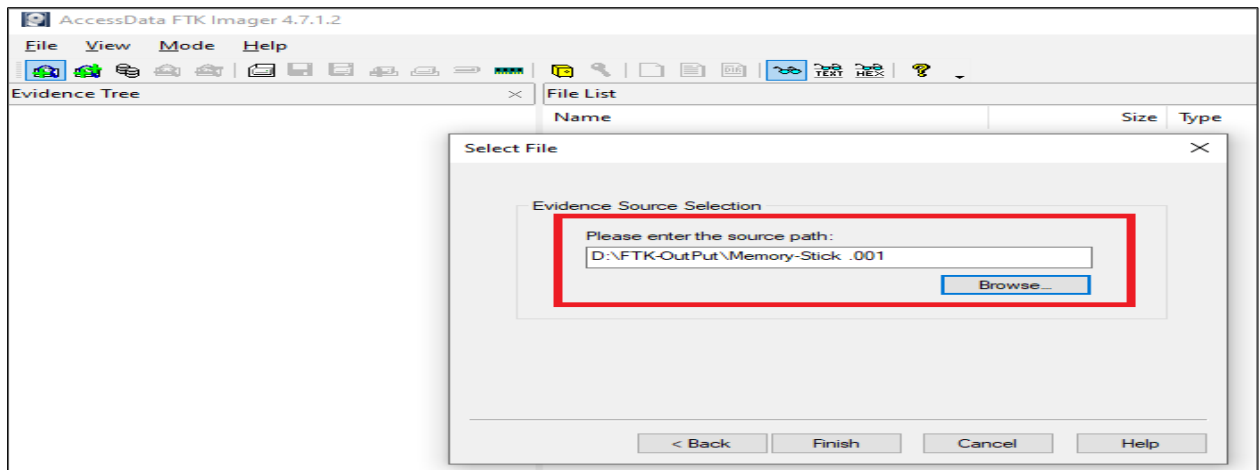
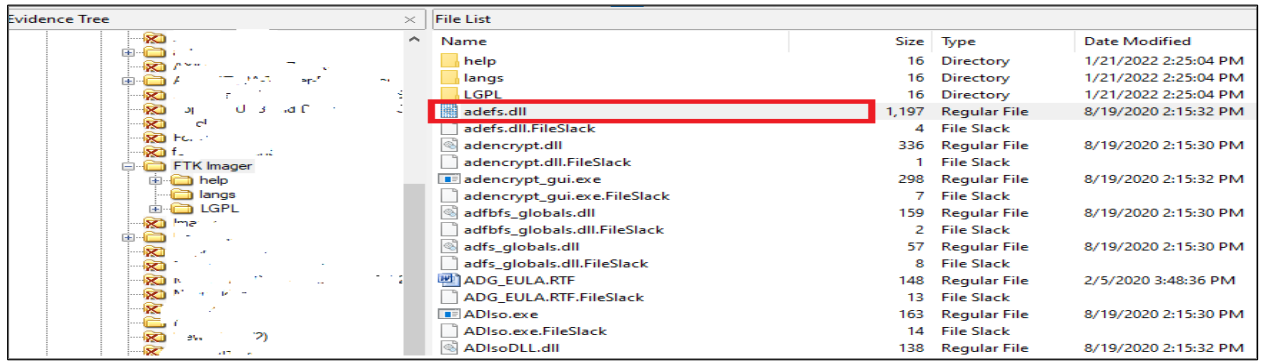
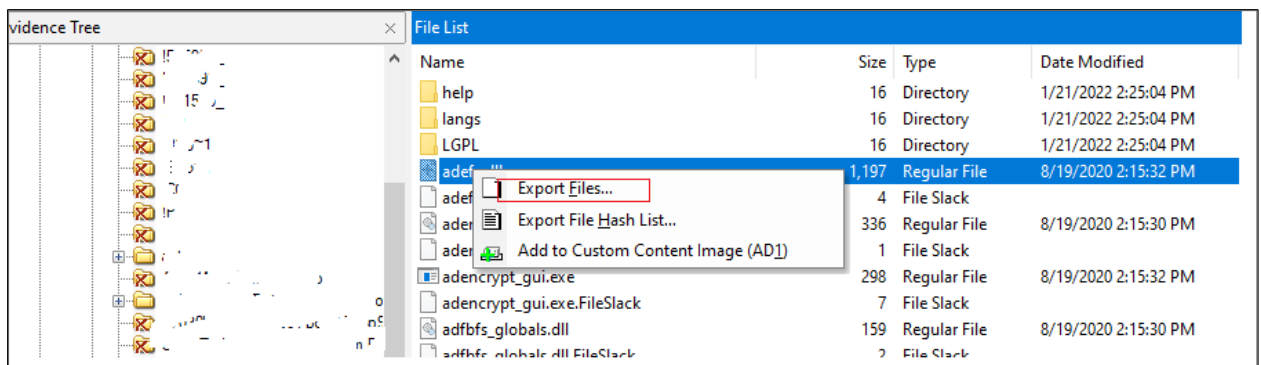


Image File Location

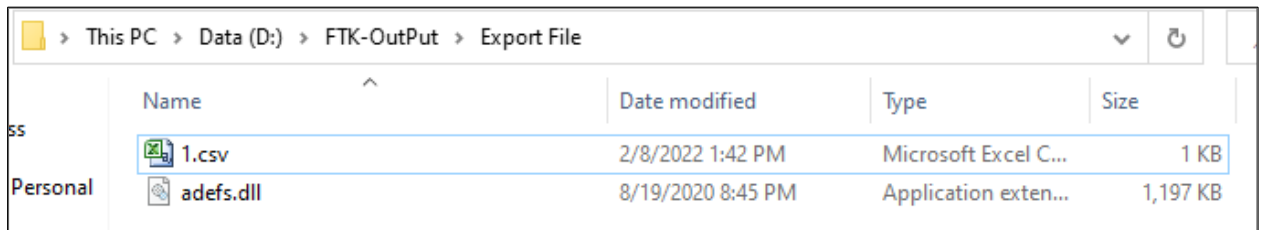
ကိုယ် Export လုပ်မဲ့ File ကိုရွေးချယ်ပြီး File ပေါ်မှာ Right Click နှိပ်ပြီး Export File ကိုရွေး၊ Export ထုတ်မဲ့နေရာကိုရွေးချယ်လိုက်ရုံပါပဲ။ File တစ်ခုထဲတင်မဟုတ်ပဲ ကျန်တဲ့ ကိုယ် လိုချင်တဲ့ File တွေကိုပါ Export လုပ်ယူနိုင်ပါတယ်။ Export File Hash List ဆိုတာ ကလဲ ကိုယ် Export လုပ်တဲ့ File ကစစ်မှန်ကြောင်း Hash Value ထုတ်ပေး တာဖြစ်ပါတယ်။



Select Export File



Export File



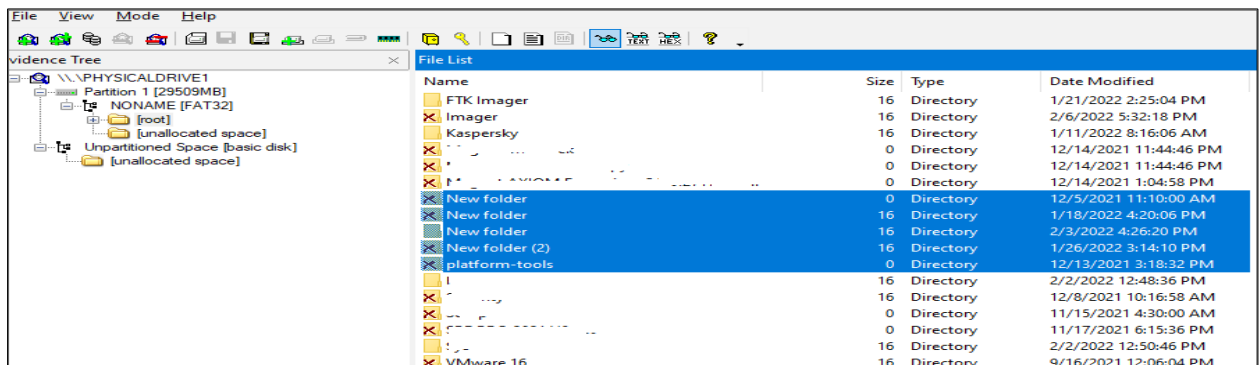
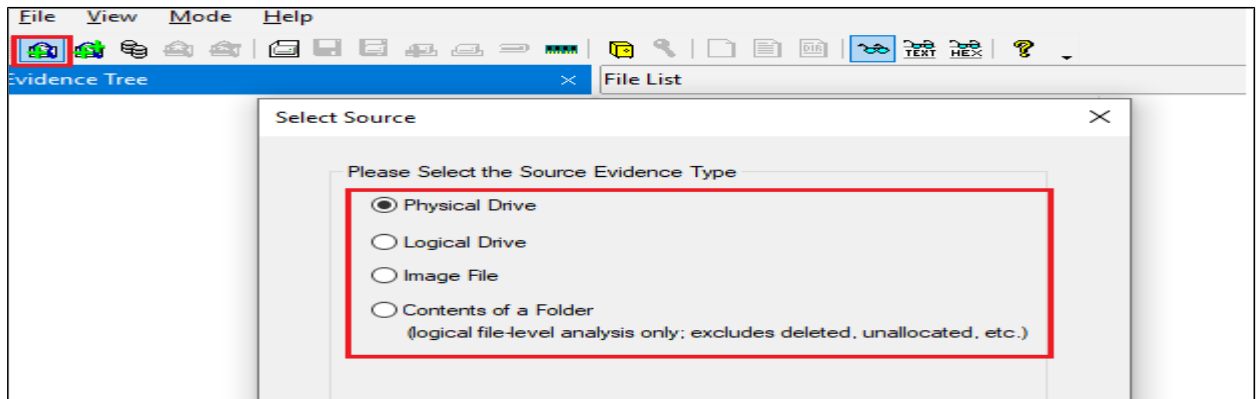
Exported File Location

Disk Or Storage Devices တွေထဲကနေ ကိုယ် Analysis လုပ်ချင်တဲ့ အပိုင်းကိုပဲ Image ပြုလုပ်ခြင်း

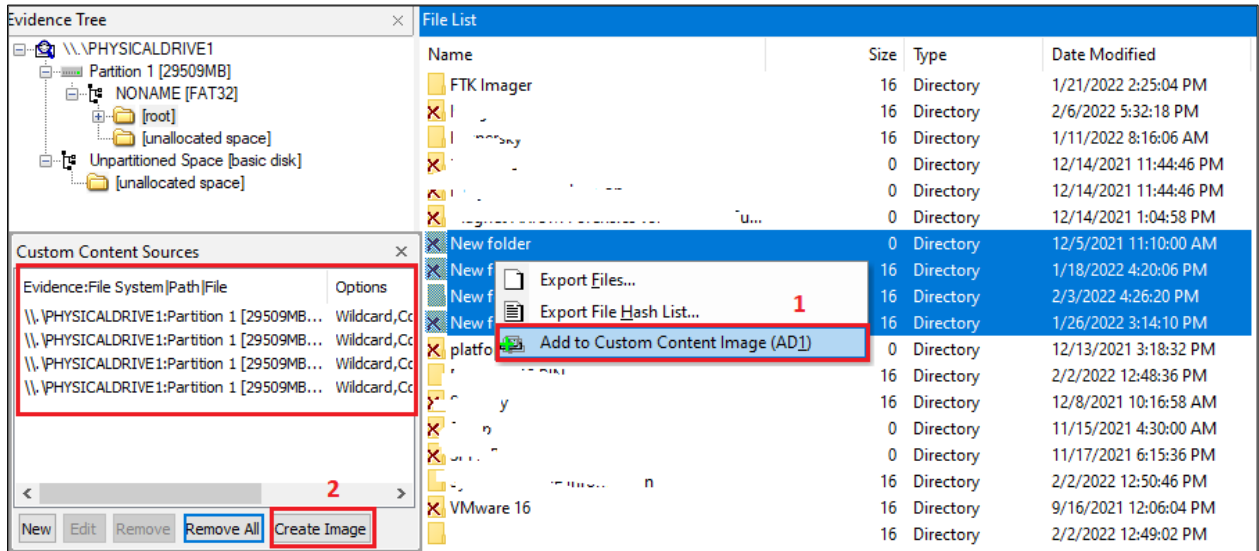
Disk Or Storage Devices တွေထဲကနေ ကိုယ် Analysis လုပ်ချင်တဲ့ အပိုင်းကိုပဲ Image ပြုလုပ်ခြင်းကို Custom Image ပြုလုပ်ခြင်းလို့လဲခေါ်ပါတယ်။ မလိုအပ်တဲ့ အပိုင်းတွေက ချန်ထားပြီး ကိုယ်လိုချင်တဲ့အပိုင်းကိုပဲ ရွေးချယ်ပြီး Forensics Image

ပြုလုပ်တာဖြစ်ပါတယ်။ အခုလို Custom Forensics Image ပြုလုပ်တဲ့အခါမှာရရှိလာမဲ့ Image Extension ကတော့ .ad1 (Access Data Image) ဖြစ်ပါတယ်။

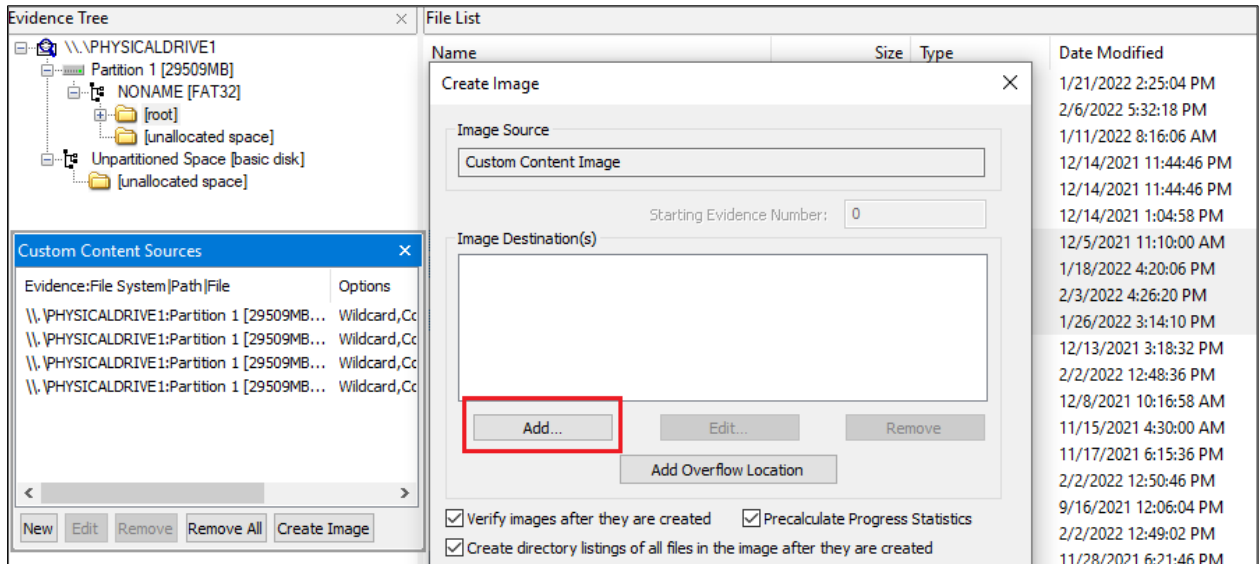
Tool Bar > Add Evidence Items ကိုနှိပ်ပြီး ကိုယ်အသုံးပြုမဲ့ Drive, Image, ကိုရွေးချယ်ပါ။ ယခုနေရာမှာ Physical Device > Memory Stick ကိုရွေးထားပါတယ်။ ရွေးပြီးတဲ့အခါမှာ Memory Stick ထဲက Data တွေကိုမြင်ရပါလိမ့်မည်။ အဲဒီအထဲမှကိုယ် Custom Image ပြုလုပ်ချင်တဲ့ Data တွေကိုရွေးယူပါ။



ကိုယ် Custom Image ပြုလုပ်မဲ့ File တွေကိုရွေးချယ်ပြီး Right Click ကိုနှိပ်ပြီး Add To Custom Content Image (AD1) ကိုရွေးချယ်ပါ။ Custom Content Sources ထဲကို Custom Image လုပ်မဲ့ File တွေရောက်ရှိသွားတာကို တွေ့ရမှာဖြစ်ပါတယ်။ Create Image ကိုနှိပ်ပြီးရင် Image လုပ်တဲ့ Process အတိုင်းဆက်သွားရင်ရပြီဖြစ်ပါတယ်။



Add To Custom Content Image (AD1)

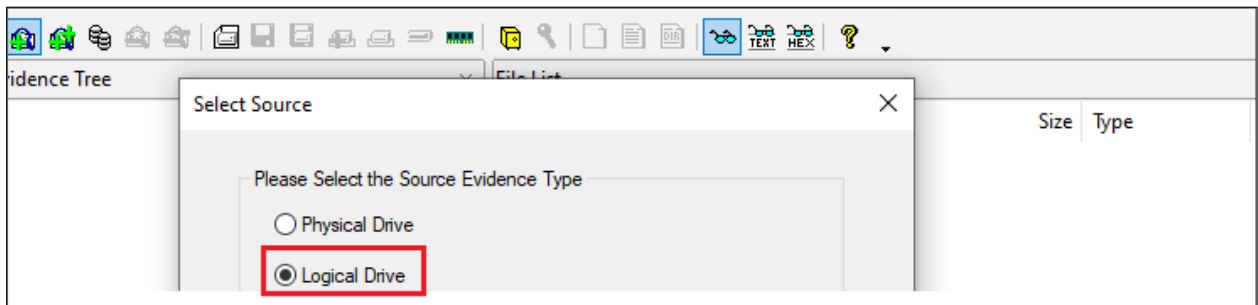
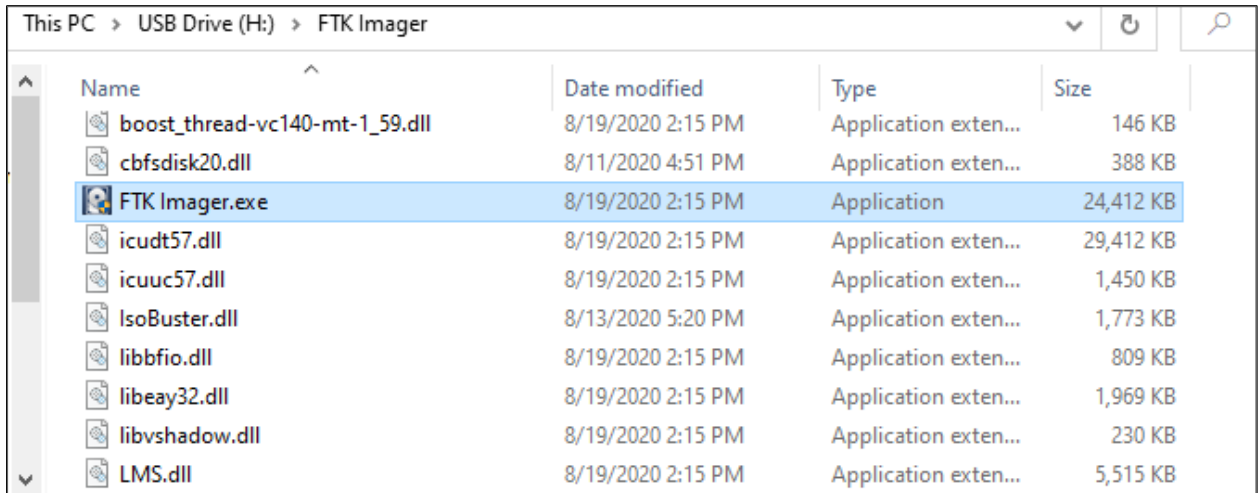


Create Forensic Image Process

System Live ဖြစ်နေတဲ့အချိန် Protected ဖြစ်နေတဲ့ System File တွေကို ရယူခြင်း

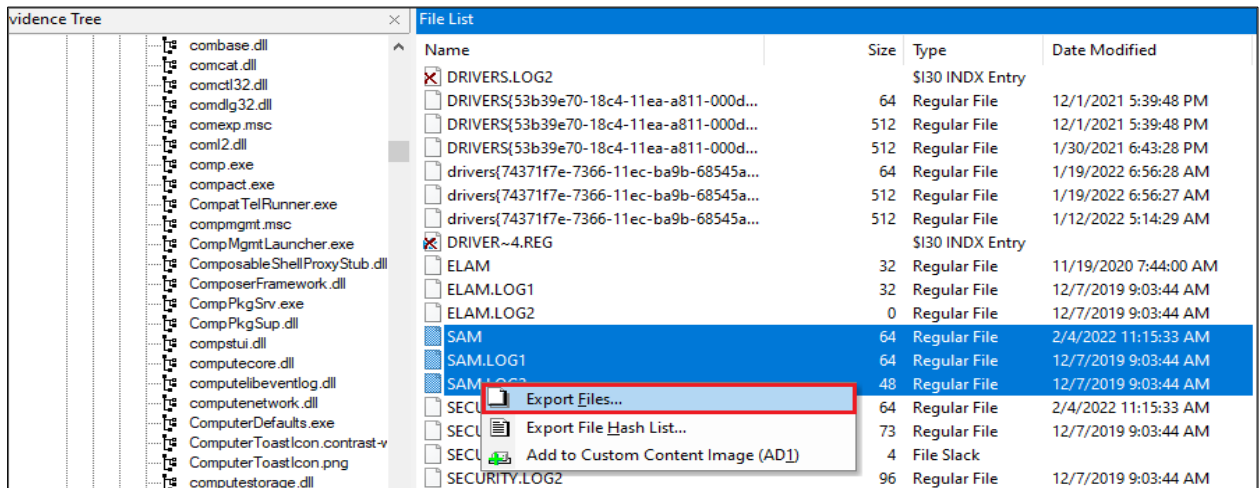
Window မှာဆိုရင် System Live ဖြစ်နေတဲ့အချိန်မှာ အချို့သော System File တွေကို Copy ပြုလုပ်လို့မရပါဘူး။ အခုနည်းလမ်းက Incident Response အတွက် အသုံးဝင်နိုင်ပါတယ်။ ဥပမာ အနေနဲ့ System File တွေဖြစ်တဲ့ Registry ထဲက SAM File ကိုယူပြထားပါတယ်။ FTK နေရာမှာ Incident Response အတွက်ဆိုရင် Kape လိုမျိုး Tool ကိုလဲအသုံးပြုနိုင်ပါတယ်။

ပထမဆုံး FTK Install ထားတဲ့ ကွန်ပျူတာထဲက Program Install Path ထဲကနေ FTK Imager ကို Copy ယူပြီး Stick ထဲကိုထည့်ထားပါတယ်။ FTK ပါတဲ့ Stick နဲ့ Live System ထဲကနေ System File ကိုရယူပါမယ်။

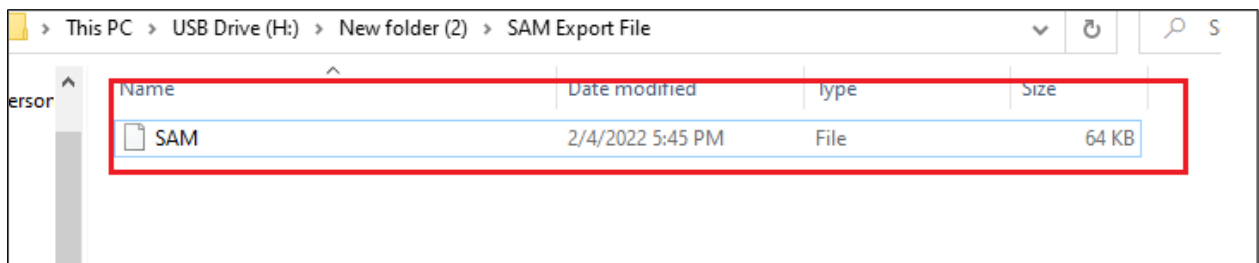


Add Evidence Items > Logical Drive

Logical Drive ကိုရွေးရတာကတော့ Registry ထဲက SAM File ကိုရယူမှာဖြစ်လို့ပါ။ Physical Drive ဆိုရင် Loading ကြာမှာစိုးတဲ့အတွက်ဖြစ်ပါတယ်။ Logical Drive ကနေ SAM File ကို Export လုပ်မှာဖြစ်တဲ့အတွက် SAM, SAM.LOG1, SAM.LOG2 File တွေကို Choice လုပ်ပြီး Export လုပ်မှာဖြစ်ပါတယ်။ SAM.LOG1, SAM.LOG2 က User ကနေမမြင်ရပါဘူး။ RAW Access နဲ့ Access လုပ်တဲ့အတွက်မြင်ရတာဖြစ်ပါတယ်။ SAM ပေါ်ကို Data တွေ Write မလုပ်ခင် ခနဲ Save ထားတဲ့ File တွေဖြစ်ပါတယ်။ Export မလုပ်ပဲ AD1 Image အနေနဲ့ Image ပြုလုပ်ရင်လဲရပါတယ်။ အခု Export လုပ်တဲ့ File ကို Stick ထဲပဲ Save ထားပါတယ်။ Export File ထဲမှာ SAM File ကိုတွေ့ရမှာဖြစ်ပါတယ်။ SAM.LOG1, SAM.LOG2 တွေကိုတော့ User က မြင်ရမှာ မဟုတ်ပါဘူး။



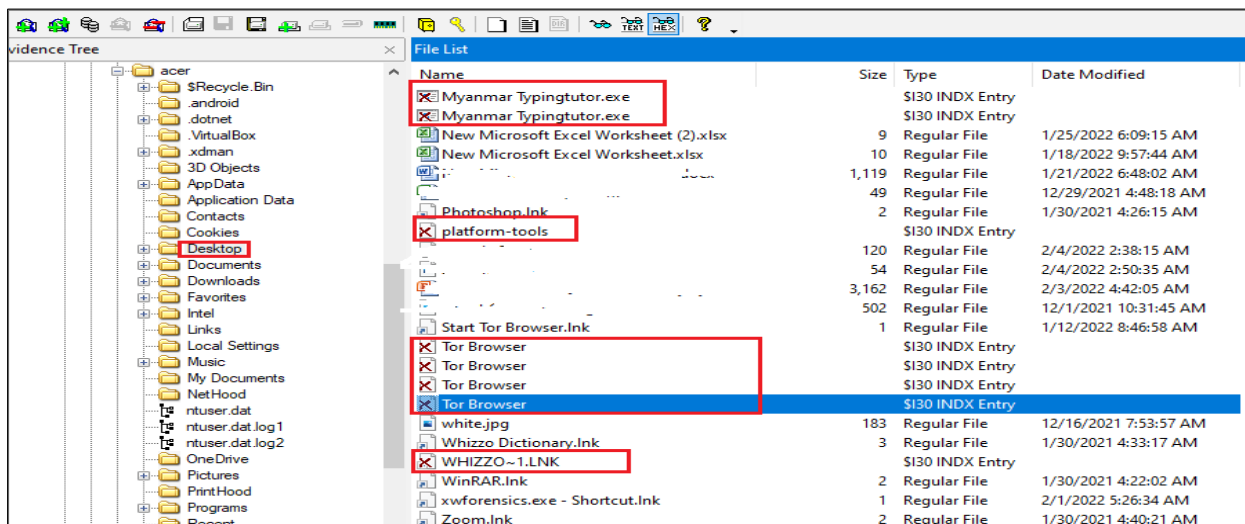
SAM File – Export



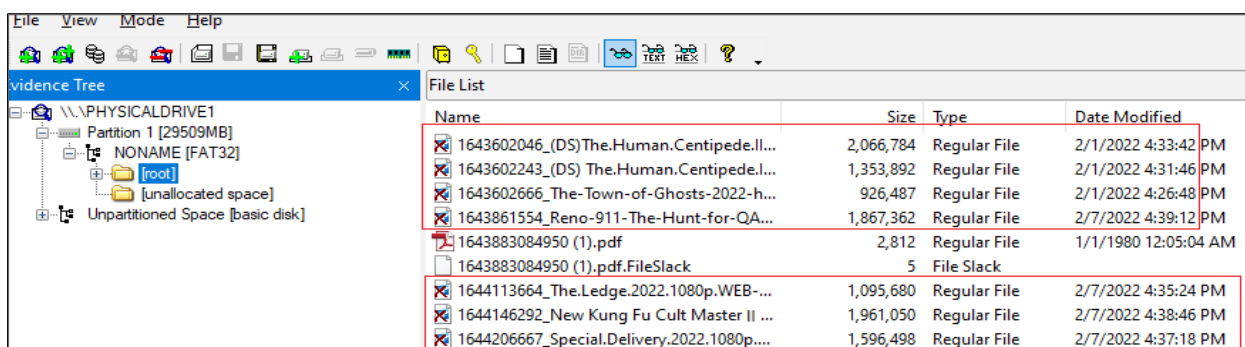
Export Folder

Image File & Storage တွေကို Analysis ပြုလုပ်ခြင်း

Storage, Image File တွေကို Detail Analysis မလုပ်ခင် FTK Imager နဲ့ Analysis ပြုလုပ်လို့ရပါတယ်။ ပထမပုံမှာ Add Evidence Items ကနေ C:\ Drive ကို Image မလုပ်ခင် မြင်ရတဲ့ အနေအထားဖြစ်ပါတယ်။ အနီရောင် ကြက်ခြေခတ်ပြထားတာတွေက ဖျက်ထားတဲ့ File တွေဖြစ်ပါတယ်။ USB Stick နဲ့ USB Stick ကို Image ရယူထားတာတွေနဲ့ ဥပမာ ပြသထားပါတယ်။ Delete လုပ်ထားတဲ့ File တွေကို ဖွင့်ကြည့်လို့မရပါ။ Raw အနေနဲ့သာ ရှိပါသေးတယ်။



C:\ Drive



USB Stick

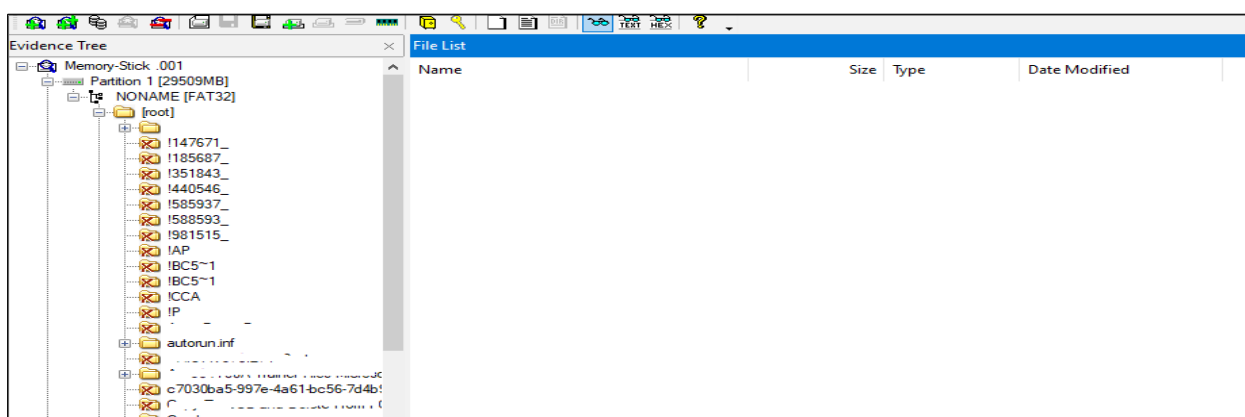
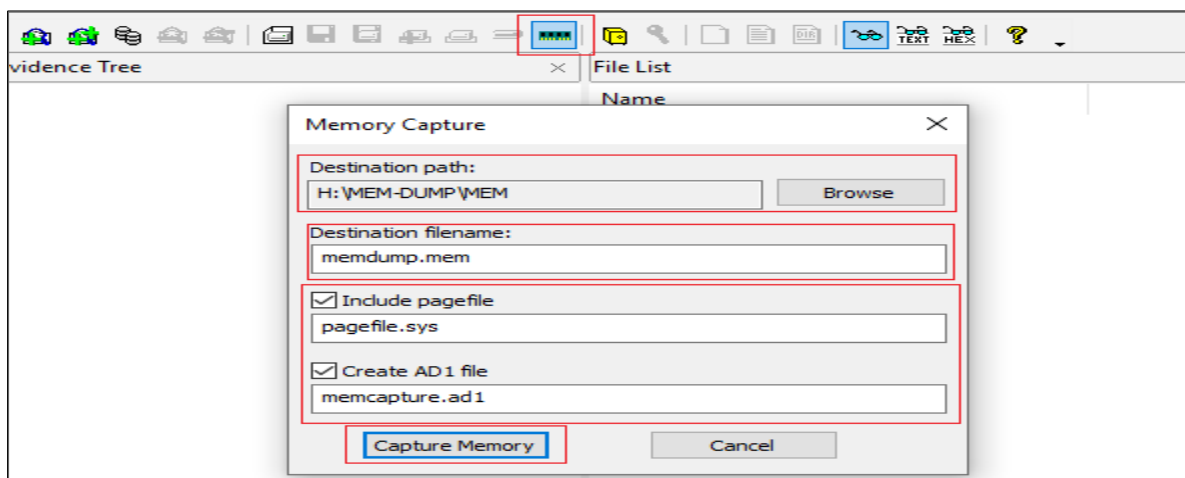


Image File – Analysis

System Live Memory Dump ရယူခြင်း

Live ဖြစ်နေတဲ့ System ကနေ Memory Image ကို FTK Imager နဲ့ရယူနိုင်ပါတယ်။ USB Stick ကနေပဲ FTK ကိုအသုံးပြုပြီး Memory Dump ပြုလုပ်မှာဖြစ်ပါတယ်။ Tool Bar > Capture Memory ကိုရွေးချယ်ပါမယ်။ Pagefile.sys ကိုပါရွေးချယ်ပြီး AD1 Image အနေနဲ့ရယူပါမယ်။ AD1 Image နဲ့မယူချင်လဲရပေမဲ့ Pagefile.sys ကိုတော့မဖြစ်မနေ ရွေးချယ်သင့်ပါတယ်။ Pagefile.sys ကလဲ Linux မှာဆို Swap သဘောမျိုးပါပဲ။ RAM က Load မနိုင်တဲ့အခါ HDD,SSD, ပေါ်မှာ သိမ်းထားတဲ့ File ဖြစ်နေတဲ့အတွက်ဖြစ်ပါတယ်။

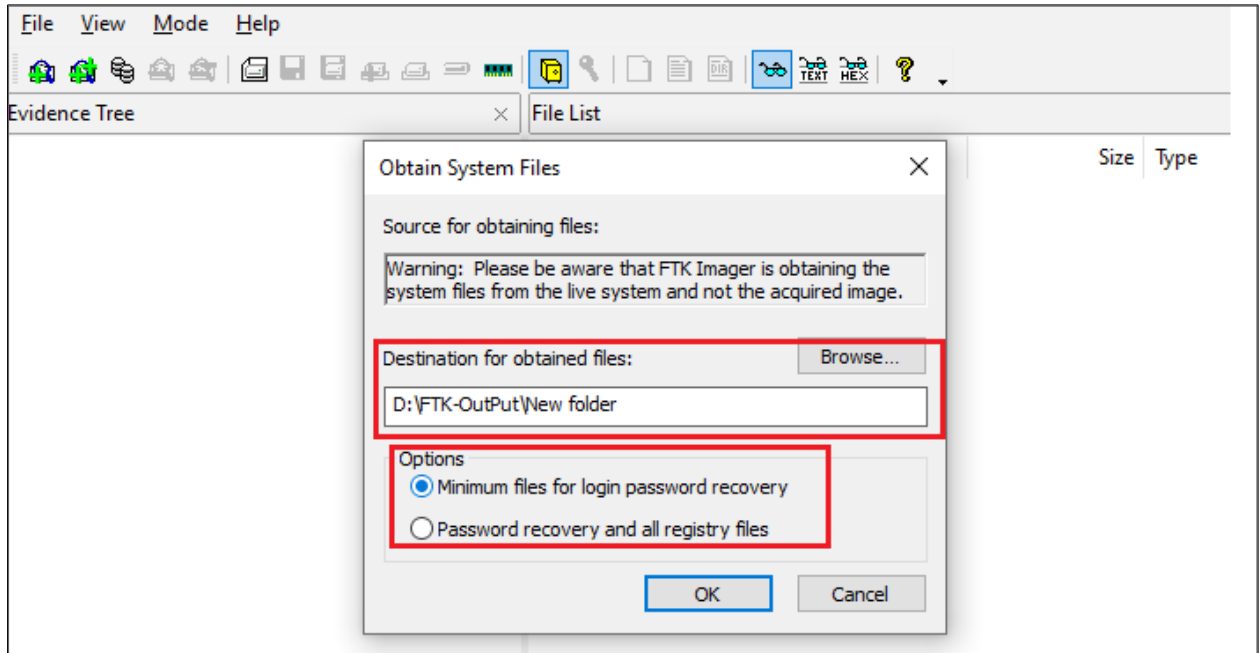


Live Ram Capture

Protected Registry Files များရယူခြင်း

Registry File တွေက System Live ဖြစ်နေတဲ့အချိန်မှာ Copy ပြုလုပ်လို့မရ နိုင်ပါ။ ထို့ကြောင့် FTK Imager ကိုအသုံးပြုပြီး Protected Registry Files တွေကိုရယူနိုင် ပါတယ်။ Protected Registry Files တွေကိုရယူရာမှာ ရွေးချယ်စရာ နည်းလမ်း ၂ ခုရှိပါတယ်။ Minimum Files For Login Recovery ဆိုတာက User Account နဲ့ပတ်သတ် တာတွေကိုရယူဖို့ Regisrty File တွေဖြစ်တဲ့ Users, System, SAM Files တွေကို ရယူတာဖြစ်ပါတယ်။ Password Recovery And All Registry Files ဆိုတာက Users, Default,SAM, Security, Software, Sytem, NTUSER.DAT File တွေကိုအကုန်ရယူ တာဖြစ်ပါတယ်။ အဲဒီအထဲကနေ User Information နဲ့ အခြား Password လုပ်ထားတဲ့ File တွေကို Recovery ရရှိနိုင်ပါတယ်။

Protected Registry Files တွေရယူဖို့အတွက် Tool Bar ကနေ Protected Registry Files ကိုနှိပ်ပြီး ကိုယ်အဆင်ပြေမဲ့နည်းလမ်းကိုရွေးချယ်ပြီးရယူနိုင်ပါတယ်။



Protected Registry Files

This PC > Data (D:) > FTK-OutPut > New folder				
Name	Date modified	Type	Size	
Users	2/8/2022 3:51 PM	File folder		
SAM	2/4/2022 5:45 PM	File	64 KB	
system	2/4/2022 5:45 PM	File	18,432 KB	

Minimum Files For Login Recovery – Output

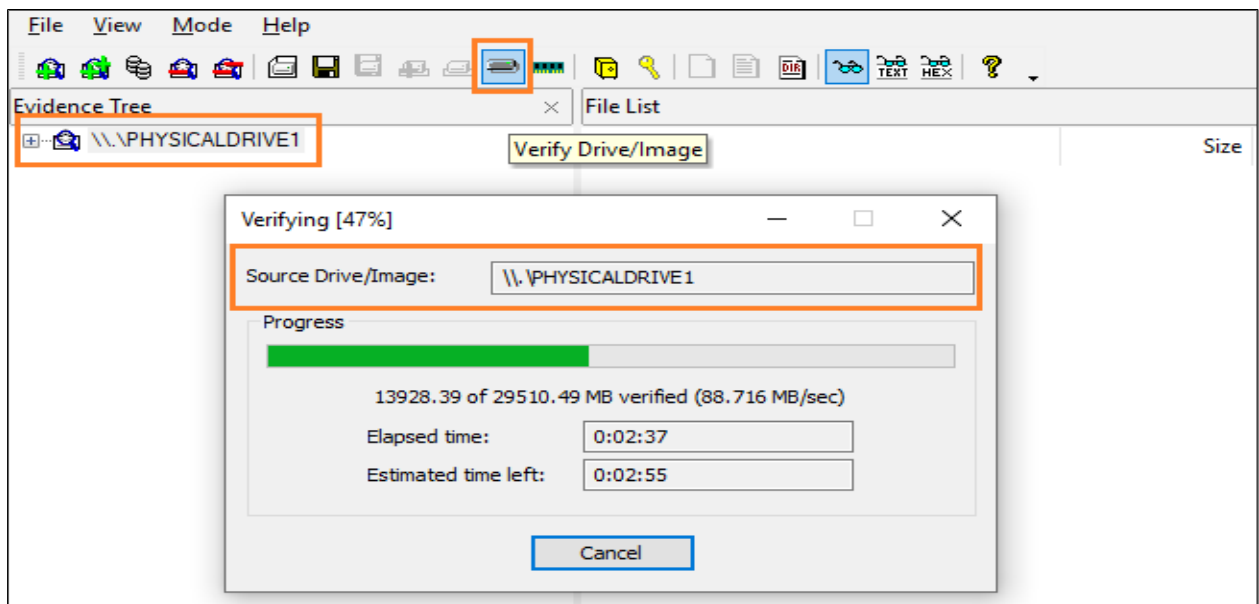
Name	Date modified	Type	Size	
Users	2/8/2022 3:19 PM	File folder		
default	2/4/2022 5:45 PM	File	512 KB	
SAM	2/4/2022 5:45 PM	File	64 KB	
SECURITY	2/4/2022 5:45 PM	File	64 KB	
software	2/4/2022 5:45 PM	File	106,240 KB	
system	2/4/2022 5:45 PM	File	18,432 KB	

Password Recovery And All Registry Files – Output

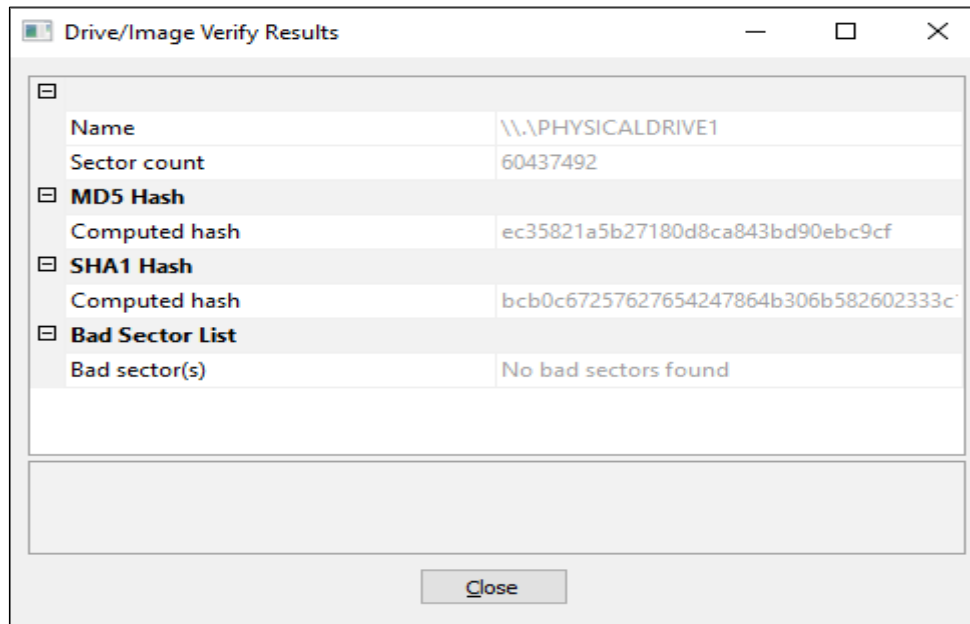
Image Integrity အတွက် Hash ပြုလုပ်နိုင်ခြင်း

Image Integrity အတွက် Hash ပြုလုပ်တယ်ဆိုတာက မူရင်း Storage Media နဲ့ Copy ဖြစ်တဲ့ Image File တို့က တူညီကြောင်း ၂ ခုစလုံးရဲ့ အထဲမှာရှိတဲ့ အချက်အလက်တွေကို ပြင်ဆင်ဖျက်ဆီးထပ်ပေါင်းထားခြင်း မရှိကြောင်းကိုပြဖို့ အတွက် Integrity ရှိအောင်ပြသတာ ဖြစ်ပါတယ်။ ဥပမာ အနေနဲ့ USB ကိုချိတ်ဆက်ပြီး Tool bar မှာရှိတဲ့ Verify Drive / Image ကိုနှိပ်ပါ။ ပထမဆုံးမူရင်း Storage ကို Verify လုပ်ပါမယ်။ ဒုတိယအနေနဲ့က မူရင်း Storage ကနေပြုလုပ်ထားတဲ့ Image File ကို Hash Verify လုပ်ပါမယ်။

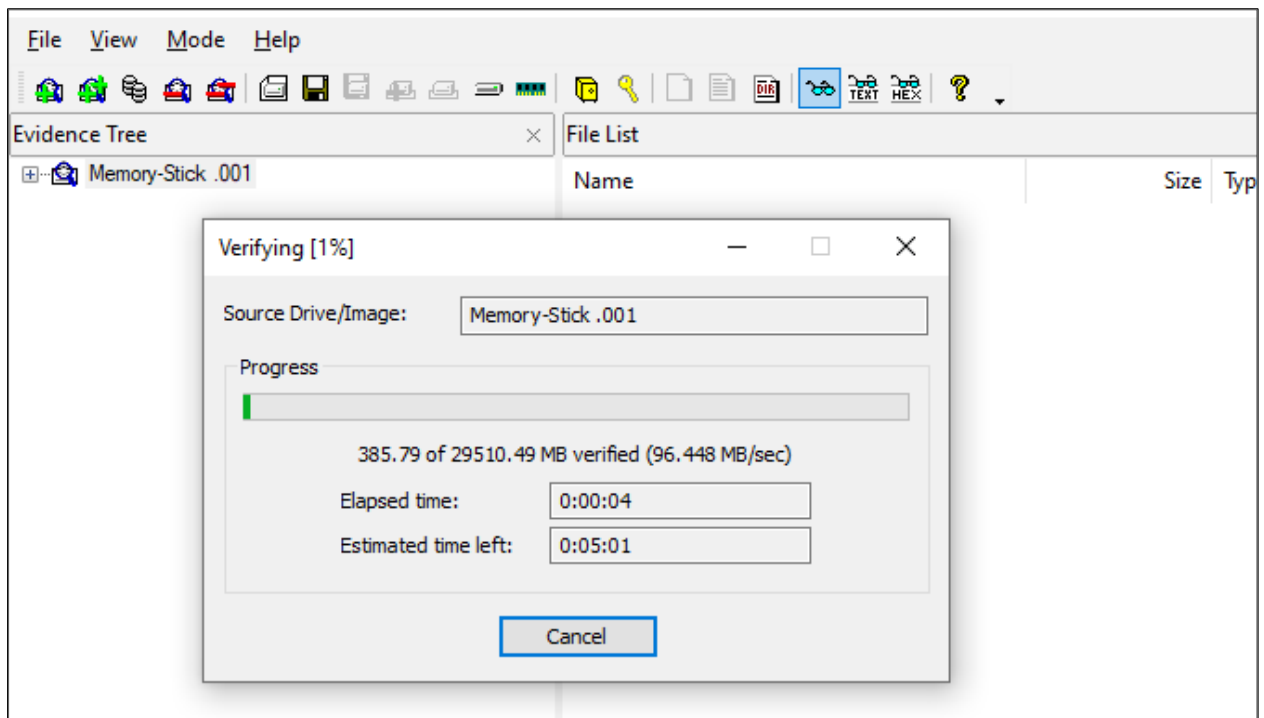
သတိထားကြည့်ရင် မူရင်း Storage ကနေ File အချို့ဖျက်ထား ပြင်ထားတဲ့အတွက် Image File က hash Value နဲ့မတူညီတာကိုသွားတွေ့ရပါမယ်။ Forensics Image File ကိုတော့ပြင် ဆင်ထားခြင်း မရှိပါဘူး။ တစ်ကယ်ဆိုရင် Image ကို Verify လုပ်ရာမှာတွေ့ရတဲ့ Computer Hash Value အတိုင်း Original Storage ရဲ့ Hash ကဖြစ်ရမှာဖြစ်ပါတယ်။ Image ကို Verify လုပ်ရာမှာ Match ဖြစ်တယ်ဆိုတာက Image မှာ တစ်စုံတစ်ခုမပြုလုပ်ထားတဲ့အတွက် ဖြစ်ပါတယ်။



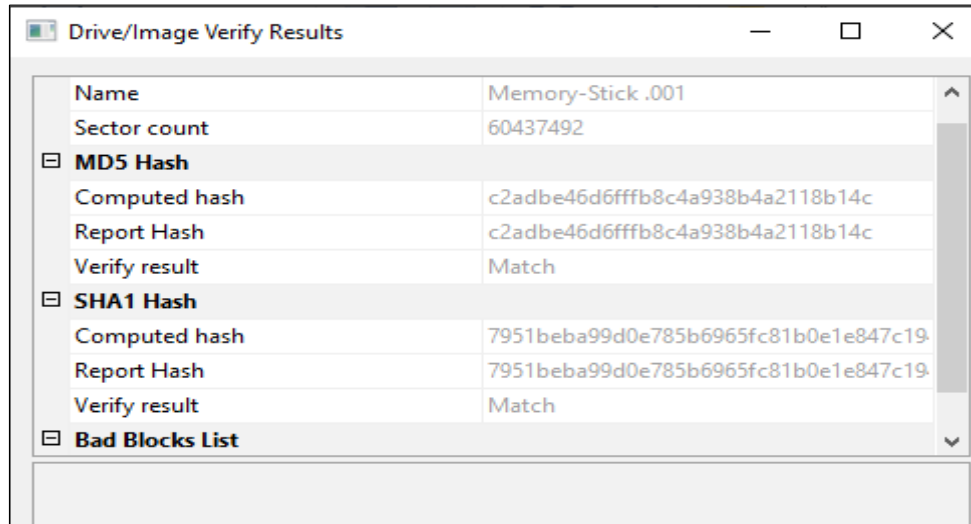
Original Storage Verify



Original Storage Hash Value



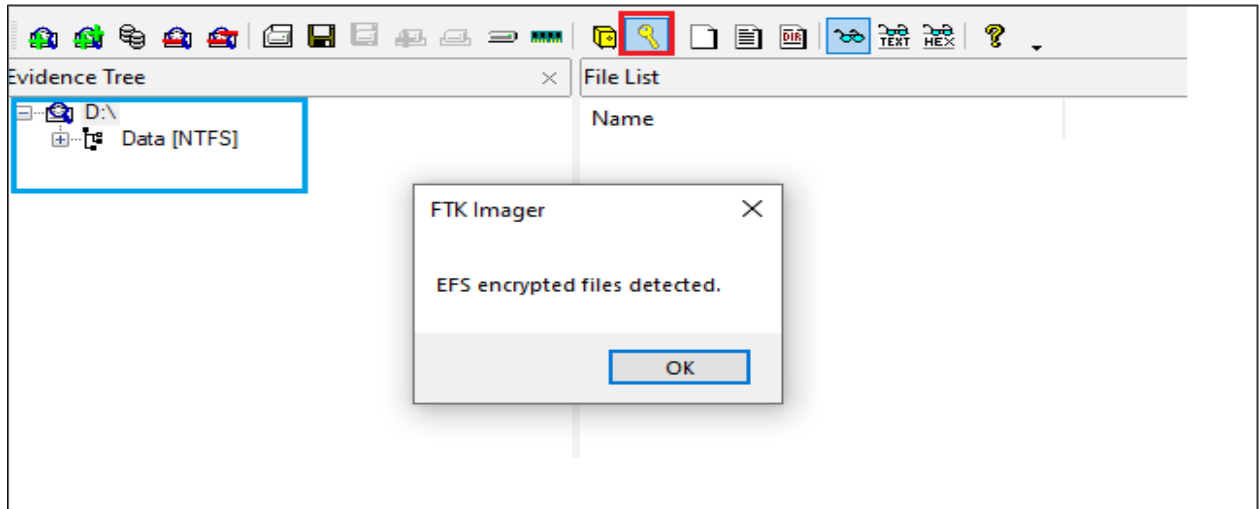
Forensics Image - Verify



Forensics Image Verify – Result

EFS Encryption ကို Detect ပြုလုပ်ခြင်း

Encryption File System - EFS Encryption ဆိုတာက Computer တစ်လုံးမှာ User တွေအများကြီးရှိတဲ့အခါမှာ User တစ်ယောက်က သူရဲ့ Folder, File တွေကိုအခြား User တွေက Access မလုပ်စေချင် တဲ့အခါမှာ အသုံးပြုပါတယ်။ EFS က NTFS File System မှာပဲ အလုပ်လုပ်ပါတယ်။ User-1 က File, Folder တစ်ခုကို EFS Encryption လုပ်ထားရင် User-2 က EFS လုပ်ထားတဲ့ Folder, File တွေကို Access လုပ်လို့မရနိုင်ပါဘူး။ ကွန်ပျူတာတစ်လုံးမှာ User အများကြီးထားရှိပြီး Bitlokcer Encryption မသုံးချင်ရင် User အများကြီးရှိနေတဲ့ အတွက် Bitlokcer ကိုအသုံးပြုလိုအဆင်မပြေရင် EFS ကိုအသုံးပြုတာ ဖြစ်ပါတယ်။ FTK Imager က EFS Encryption ကို Detect လုပ်ပေးနိုင်ပါတယ်။ ဥပမာ အနေနဲ့ D:\ ထဲမှာ EFS Folder တစ်ခုလုပ်ထားပါတယ်။ Drive D:\ ကို FTK Imager ကနေ Add Evidence Item လုပ်ပြီးတဲ့အချိန်မှာ EFS Encryption ရှိ - မရှိ ကိုကြည့်နိုင်ပါတယ်။

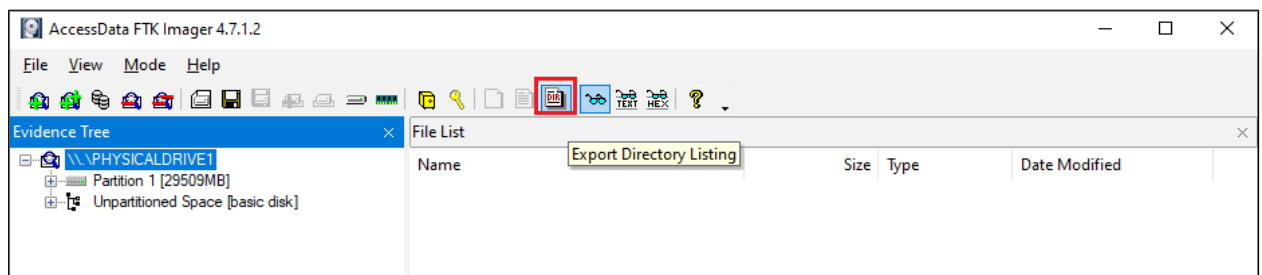


EFS Encryption Detect

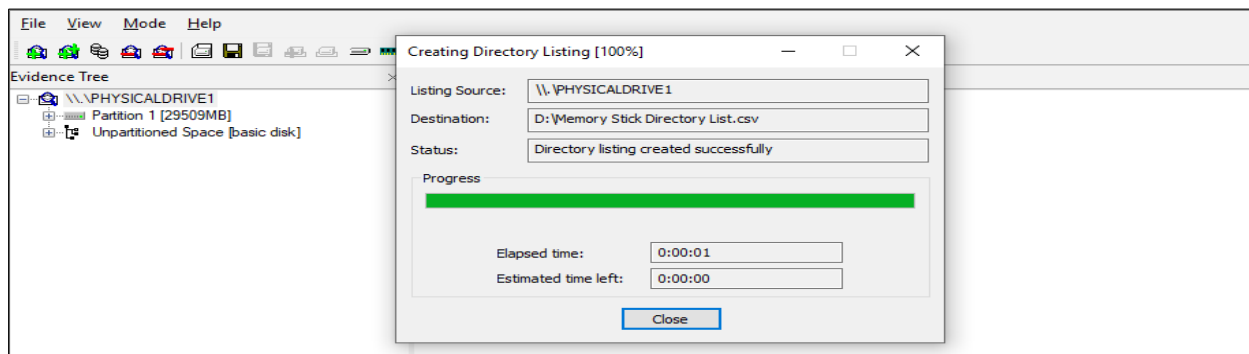
အခြားသော Feature များ

Export Directory Listing

Add Evidence Items ကိုနှိပ်ပြီး Storage Media တစ်ခုကိုထည့်ပါ။ Storage Media က FTK Imager ထဲကိုရောက်တာနဲ့ Storage ပေါ်ကို Right Click နှိပ်ပြီး Export Directory Listing ကိုရွေးကာ Storage ထဲမှာရှိတဲ့ File List တွေကို Export ထုတ်ယူနိုင်ပါတယ်။ Export Directory Listing အကြောင်းကအပေါ်မှာလဲရေးထားပြီးသားဖြစ်ပါတယ်။ ကိုယ့်လုပ်ငန်း အခြေအနေနှင့် လိုအပ်ချက်အပေါ်မူတည်ပြီးလုပ်ဆောင်နိုင်ပါတယ်။ အသုံးပြု တာများရင် အဆင်ပြေ သွားမှာဖြစ်ပါတယ်။ Excel Output File မှာဆိုရင် File Name, File Location, File Size, File Creat Date, File Access Date, File (Delete Status) တို့ကိုတွေ့နိုင်ပါတယ်။



Export Directory Listing



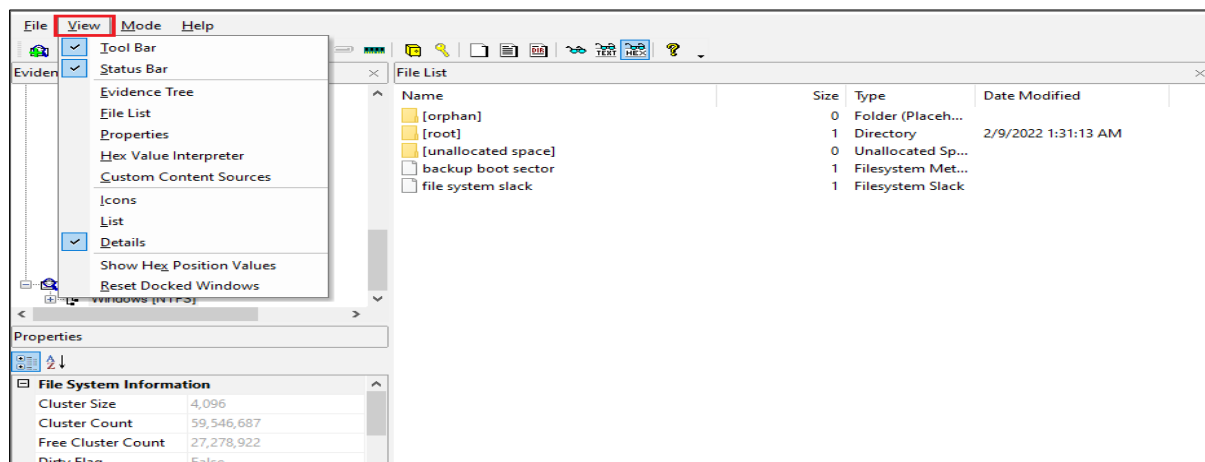
Export Directory Listing

	A	B	C	D	E	F	G
	Filename	Full Path	Size (bytes)	Created	Modified	Accessed	Is Deleted
1	Imager.docx	Partition 1\NONAME [FAT32]\[root]\Imager.docx	4327284	022-Feb-08 16:30:14.25000	2022-Feb-08 16:28:18		no
2	EFS key.pfx	Partition 1\NONAME [FAT32]\[root]\EFS key.pfx	2558	022-Feb-09 08:15:33.66000	2022-Feb-09 08:15:40		no
3	New folder	Partition 1\NONAME [FAT32]\[root]\New folder\	0	022-Feb-09 08:16:13.29000	2022-Feb-09 08:16:14		yes
4	!64411*1.MP4	Partition 1\NONAME [FAT32]\[root]\!64411*1.MP4	1144324942	022-Feb-08 16:33:47.65000	2022-Feb-07 16:35:26		yes
5	1644112999_Turner and Hooch 1989 720p (CM).mp4	1\NONAME [FAT32]\[root]\1644112999_Turner and Hooch 1989 720p (CM).mp4	1201499609	022-Feb-08 16:40:25.56000	2022-Feb-08 16:57:04		yes

Export Directory Listing – Excel

View Mode

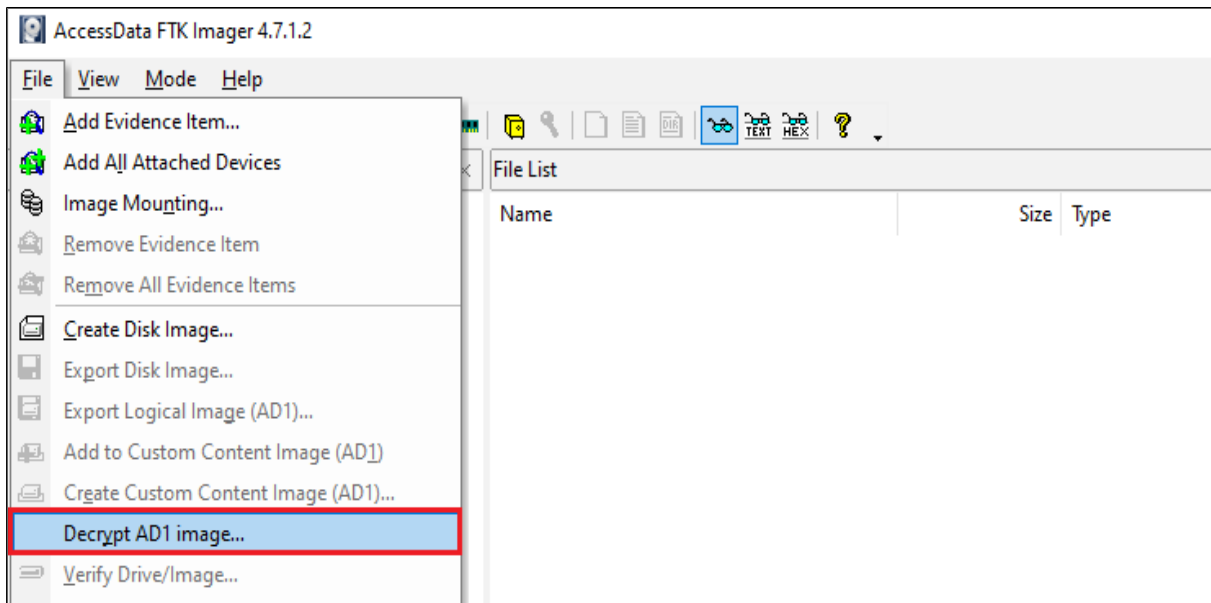
View Mode ကနေ ကိုယ်လိုချင်တဲ့ပုံစံမျိုးဖြစ်အောင်ပြောင်းလဲနိုင်ပါတယ်။



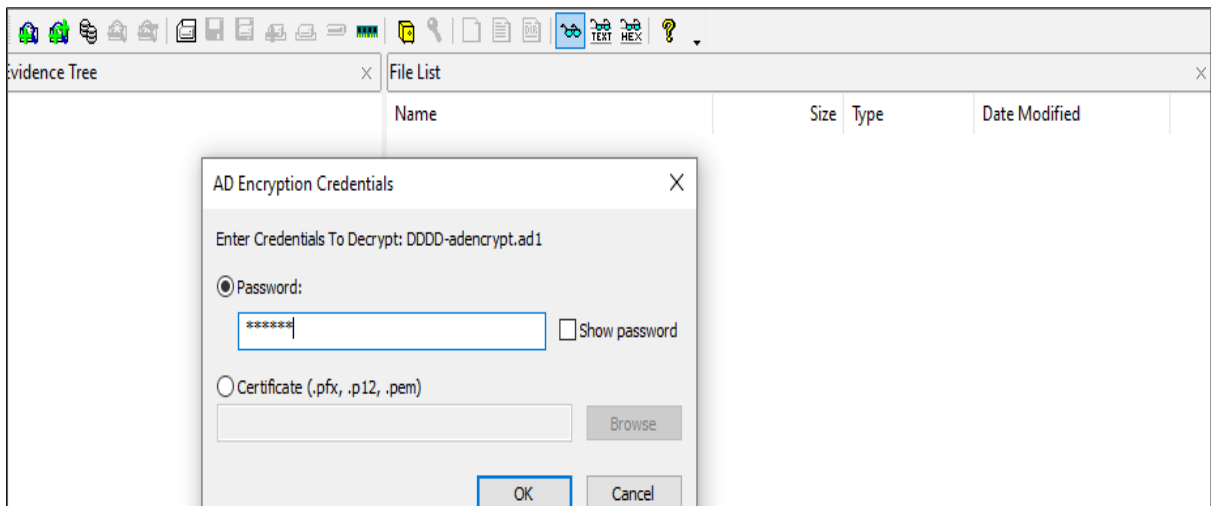
View Mode

Decrypt AD1 Image

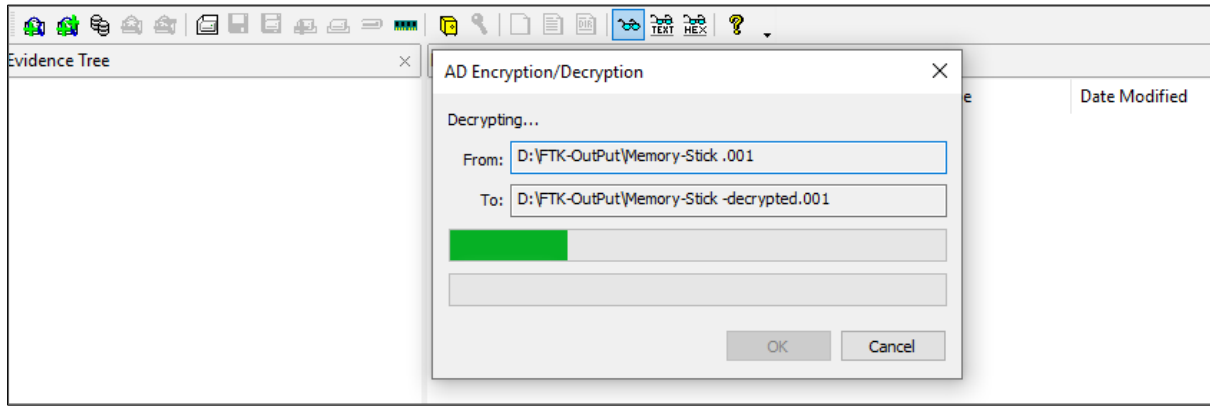
Decrypt AD1 Image ကတော့ Password ပေးထားတဲ့ Forensics Image File ကို Decrypt လုပ်ဖို့အတွက်အသုံးပြုတာဖြစ်ပါတယ်။ Add Evidence Items ကနေလဲ Password ပေးထားတဲ့ Image File ကို Decrypt လုပ်လို့ရပါတယ်။ Image File ရှိတဲ့နေရာ ကိုထည့်ပြီး ပေးထားတဲ့ Password ကို ထည့်လိုက်ရုံပဲဖြစ်ပါတယ်။



Decrypt AD1 Image



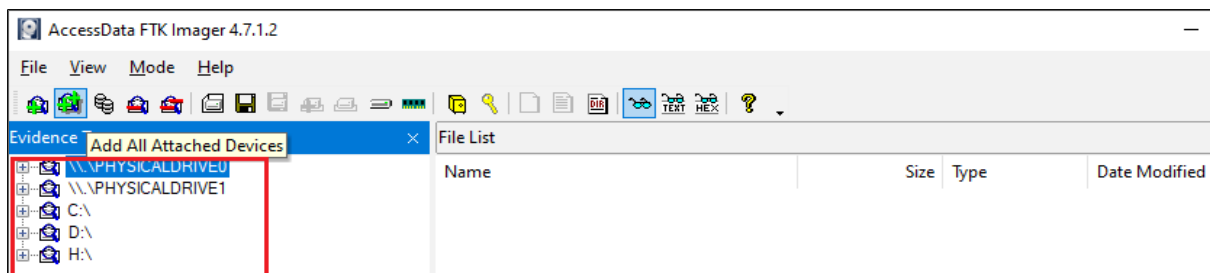
Enter Your Password For Image



Decrypting Forensics Image

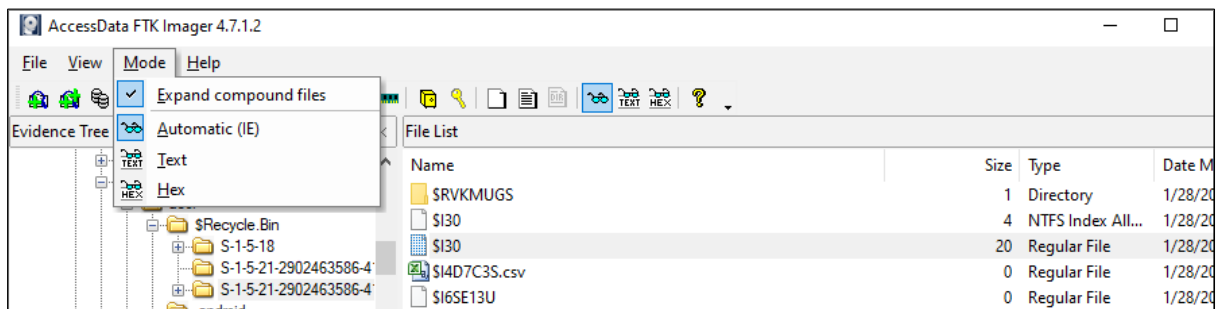
Add All Attached Devices

Add All Attached Devices ကတော့ System မှာရှိနေတဲ့ Storage အားလုံးကို FTK Imager မှာပေါ်လာအောင်ပြုလုပ်တာဖြစ်ပါတယ်။

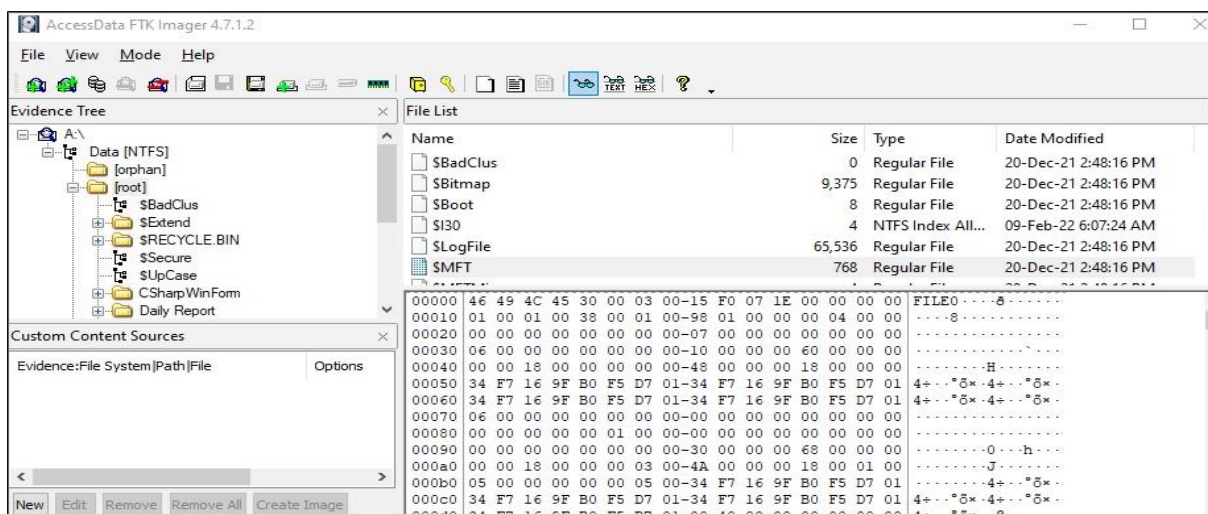


Add All Attached Devices

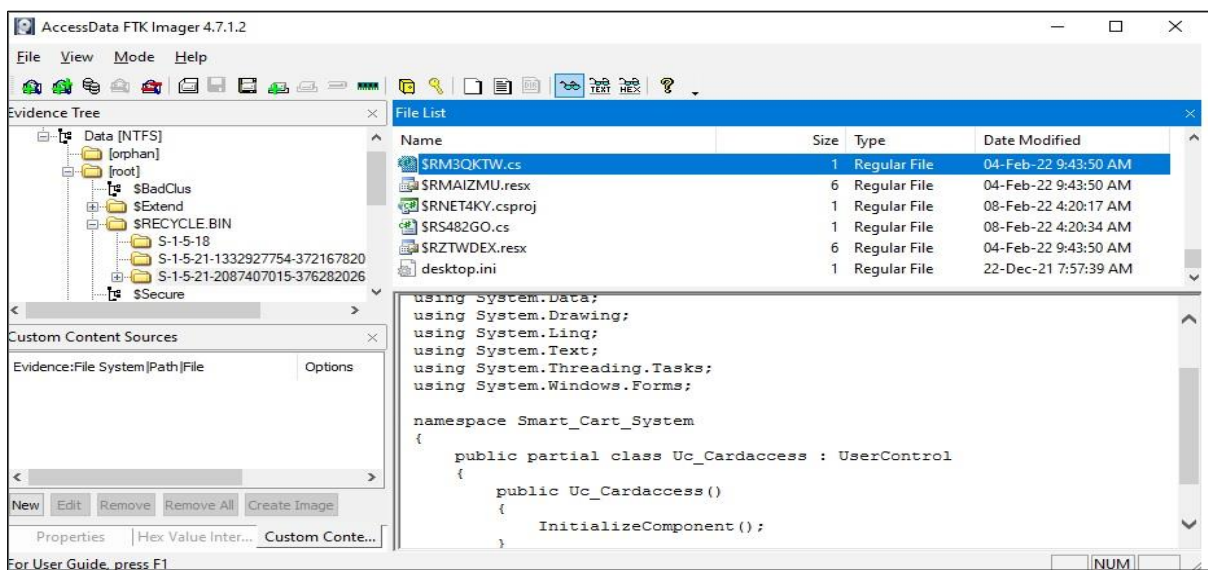
FTK Imager မှာ Evidence အပ်ပြီးရင် Data တွေကိုကြည့်ဖို့အတွက် Preview Mode 3 ခုရှိပါတယ်။ Automatic mode, Text mode, Hex mode တို့ဖြစ်ပါတယ်။ Automatic Mode ကတော့ ကိုယ်ကြည့်ရမည့် Data နဲ့ကိုက်ညီမဲ့ Format နဲ့ Automatic ပြသပေးပါတယ်။ Web pages, Web-related graphics (JPEGs GIFs) နဲ့ အခြား Media Format တွေကို IE Plugin နဲ့ပြသပေးပါတယ်။ Text View မှာတော့ ASCII or Unicode characterse နဲ့ပြသပေးပါတယ်။ Hex Mode ကတော့ Hex Value အနေနဲ့ကြည့်နိုင်ပါတယ်။ FTK Imager က Support မပေးတဲ့ Format တွေဆိုရင် ကြည့်မည့် File ကို Export ထုတ်ပြီး ကိုယ်ညီမဲ့ Viewerနဲ့ကြည့်နိုင်ပါတယ်။



Preview Mode

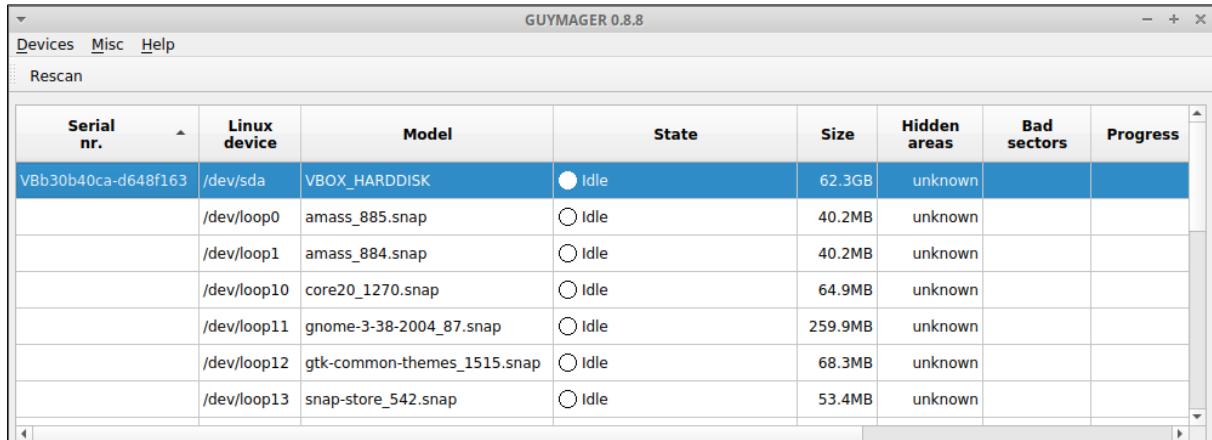


Hex View

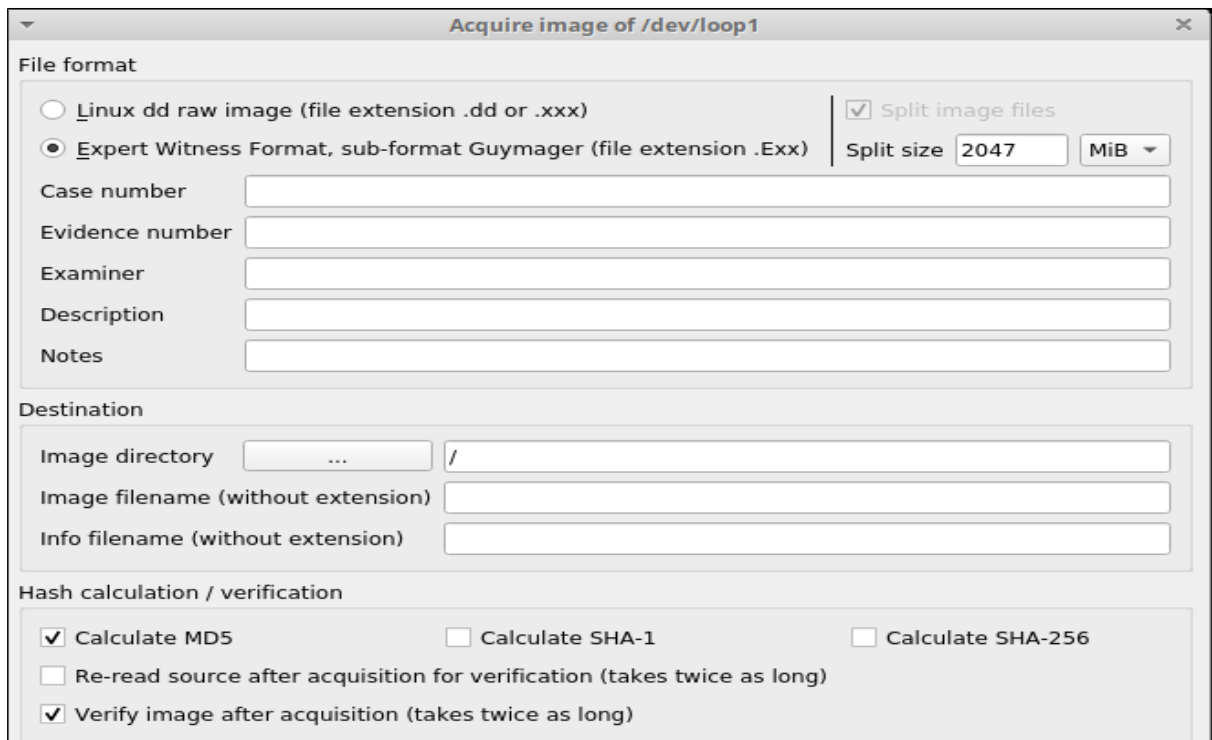


Text View

Open Source Imager နောက်တစ်ခုကတော့ Linux မှာအသုံးပြုတဲ့ Guy Mager ပဲဖြစ်ပါတယ်။ အသုံးပြုပုံတွေက FTK Imager နဲ့ဆင်တူပါတယ်။



GuyMager Main Menu



GuyMager Acquire Image Menu

အခုလောက်ဆိုရင် Digital Forensics ရဲ့ Acquisition Process တွေကို အတော် အသင့်နားလည်သဘောပေါက်ပြီဖြစ်ပါတယ်။ နိုင်ငံတွေအလိုက်နည်းစနစ်တွေကွဲပြားမှုရှိပေမဲ့ တော်တော်များများကတော့ လုပ်ပုံလုပ်နည်း သဘောတရားတွေမှာတူညီပါတယ်။ FTK - Imager ကိုအသုံးပြုတတ် Acquisition Process ကိုနားလည်မယ်ဆိုရင် မည်သည့် Forensics Hardware၊ Softwar Imager တွေကိုသုံးရသည်ဖြစ်စေ အလွယ်တစ်ကူအသုံးပြု နိုင်မှာဖြစ်ပါတယ်။

ခင်မင်လေးစားလျှက်

Aung Zaw Myo (ThirdEye)